導入ガイドラインとストレージのベストプラクティス

Enterprise applications

NetApp
May 03, 2024

目次

導入ガイドラインとストレージのベストプラクティス

概要

Microsoft Windows Serverは、ネットワーク、セキュリティ、仮想化、プライベートクラウド、ハイブリッドクラウド、 仮想デスクトップインフラ、アクセス保護、情報保護、Webサービス、アプリケーションプラットフォームインフラ、 その他多数。

このドキュメントは、以前に公開されていたテクニカルレポート**_TR-4568：『NetApp Deployment Guidelines and Storage Best Practices for Windows Server_』**の内容を置き換えます。

NetApp ONTAP®管理ソフトウェアは、**NetApp**ストレージコントローラ上で動作します。複数の形式で使用できます。

- ファイル、オブジェクト、ブロックの各プロトコルをサポートするユニファイドアーキテクチャ。これにより、ストレージコントローラがNASデバイスとSANデバイスの両方、およびオブジェクトストアとして機能できるようになります。
- ブロックプロトコルのみに重点を置き、接続ホストに対称アクティブ/アクティブマルチパスを追加することでI/O再開時間（IORT）を最適化するオールSANアレイ（ASA）
- ソフトウェア定義型のユニファイドアーキテクチャ
  - VMware vSphereまたはKVMで実行されるONTAP Select
  - クラウドネイティブインスタンスとして実行されるCloud Volumes ONTAP
- ハイパースケールクラウドプロバイダが提供するファーストパーティ製品
  - NetApp ONTAP 対応の Amazon FSX
  - Azure NetApp Files の特長
  - Google Cloud NetAppボリューム

ONTAPは、NetApp Snapshot（R）テクノロジ、クローニング、重複排除、シンプロビジョニング、シンレプリケーションなどのNetApp Storage Efficiency機能を提供 圧縮、バーチャルストレージ階層化など、パフォーマンスと効率性が向上しています。

Windows ServerとONTAPを併用すれば、大規模な環境でも運用でき、データセンターの統合やプライベートクラウドやハイブリッドクラウドの導入に大きな価値をもたらすことができます。また、この組み合わせにより、システムを停止することなくワークロードを効率的に実行でき、シームレスな拡張性

対象読者

本ドキュメントは、Windows Server向けのNetAppストレージソリューションを設計するシステムアーキテクトおよびストレージアーキテクトを対象としています。

本ドキュメントでは、次のことを前提としています。

- NetAppのハードウェアおよびソフトウェアソリューションに関する一般的な知識がある。を参照してください "システムアドミニストレーションガイド（クラスタ管理）" を参照してください。

- iSCSI、FC、ファイルアクセスプロトコルSMB / CIFSなどのブロックアクセスプロトコルに関する一般的な知識がある読者。を参照してください "clustered Data ONTAPのSAN管理" を参照してください。を参照してください "NAS管理" を参照してください。
- 読者には、Windows Server OSおよびHyper-Vに関する一般的な知識があります。

テスト済みでサポートされているSANおよびNAS構成のマトリックスについては、定期的に更新される完全なマトリックスを参照してください。 "Interoperability Matrix Tool （ IMT ）" NetApp Support Site上。IMTを使用すると、特定の環境でサポートされている製品や機能のバージョンを確認できます。NetApp IMTには、NetAppでサポートされる構成と互換性のある製品コンポーネントとバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

NetAppストレージおよびWindows Server環境

に記載されているように "概要"NetAppストレージコントローラは、ファイル、ブロック、オブジェクトの各プロトコルをサポートする真のユニファイドアーキテクチャを提供します。これには、SMB / CIFS、NFS、NVMe/TCP、NVMe/FC、iSCSI、 FC（FCP）とS3が統合され、クライアントとホストのアクセスが統合されます。同じストレージコントローラで、NFSやSMB / CIFSと同様にSAN LUNとファイルサービスという形式のブロックストレージサービスを同時に提供できます。ONTAPは、iSCSIおよびFCPとの対称アクティブ/アクティブマルチパスによってホストアクセスを最適化するオールSANアレイ（ASA）としても利用できますが、Unified ONTAPシステムでは非対称アクティブ/アクティブマルチパスが使用されます。どちらのモードでも、ONTAPはNVMe over Fabrics（NVMe-oF）マルチパス管理にANAを使用します。

ONTAPソフトウェアを実行するNetAppストレージコントローラは、Windows Server環境で次のワークロードをサポートします。

- 継続的可用性を備えたSMB 3.0共有でホストされるVM
- iSCSIまたはFCで実行されているCluster Shared Volume（CSV；クラスタ共有ボリューム）LUNでホストされているVM
- SMB 3.0共有上のSQL Serverデータベース
- NVMe-oF、iSCSI、FC上のSQL Serverデータベース
- その他のアプリケーションワークロード

さらに、NetApp重複排除、NetApp FlexClone（R）コピー、NetApp Snapshotテクノロジ、シンプロビジョニング、圧縮、 また、ストレージ階層化は、Windows Serverで実行されるワークロードに大きな価値をもたらします。

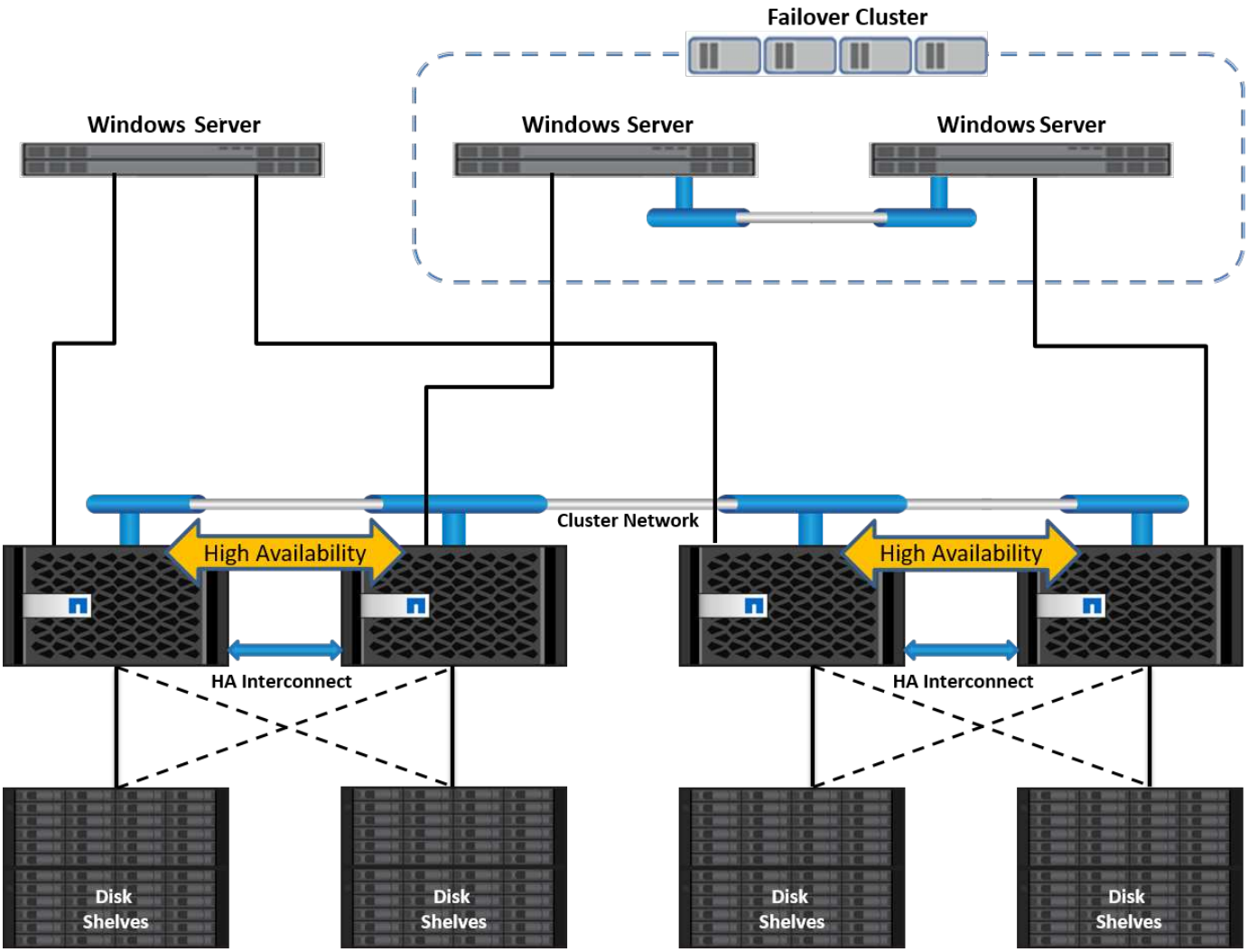
ONTAPデータ管理

ONTAPは、NetAppストレージコントローラ上で実行される管理ソフトウェアです。NetAppストレージコントローラはノードと呼ばれ、プロセッサ、RAM、NVRAMを搭載したハードウェアデバイスです。ノードは、SATA、SAS、SSDのディスクドライブ、またはそれらのドライブの組み合わせに接続できます。

複数のノードが1つのクラスタシステムに集約されます。クラスタ内のノードは相互に継続的に通信し、クラスタのアクティビティを調整します。2つの10Gbイーサネットスイッチで構成される専用のクラスタネットワ

ークへの冗長パスを使用することで、ノード間でデータを透過的に移動することもできます。クラスタ内のノードが相互にテイクオーバーして、フェイルオーバー時の高可用性を実現できます。クラスタは、ノード単位ではなくクラスタ全体が1つの単位として管理され、データは1つ以上のStorage Virtual Machine（SVM）から提供されます。クラスタからデータを提供するには、少なくとも1つのSVMが必要です。

クラスタの基本単位はノードで、ノードはハイアベイラビリティ（HA）ペアの一部としてクラスタに追加されます。HAペアは、（専用のクラスタネットワークから分離された）HAインターコネクトを介して相互に通信し、HAペアのディスクへの接続を冗長化することで、高可用性を実現します。シェルフにはHAペアのどちらかのメンバーに属するディスクが含まれている場合もありますが、HAペア間でディスクが共有されることはありません。次の図は、Windows Server環境におけるNetAppストレージの導入を示しています。

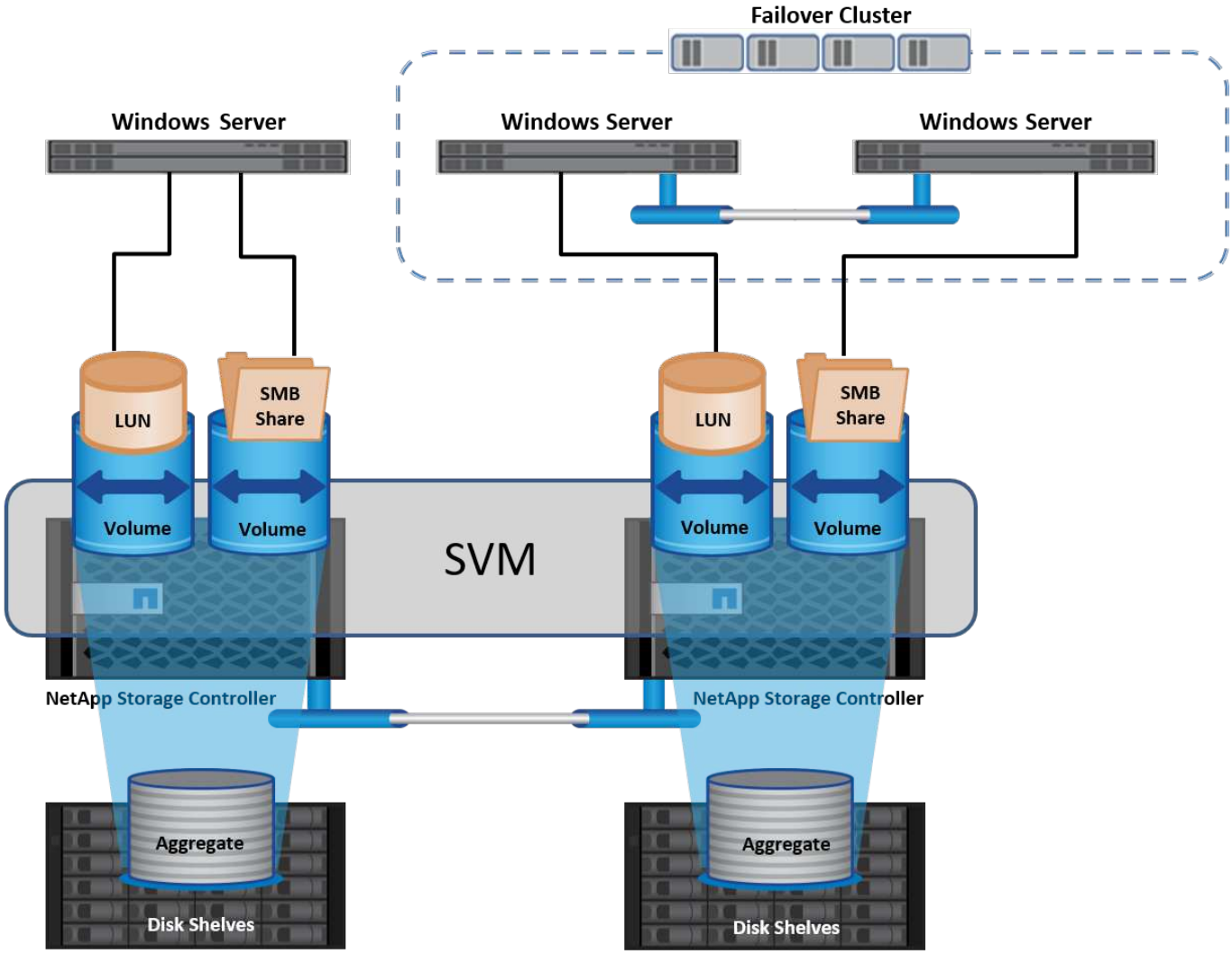


Storage Virtual Machine

ONTAP SVMは、1つ以上の論理インターフェイス（LIF）からLUNやNASネームスペースへのデータアクセスを提供する論理ストレージサーバです。したがって、SVMはストレージセグメント化の基本単位であり、ONTAPでセキュアマルチテナンシーを実現します。各SVMは、物理アグリゲートからプロビジョニングされた専用のストレージボリュームと、物理イーサネットネットワークまたはFCターゲットポートに割り当てられた論理インターフェイス（LIF）で構成されます。

論理ディスク（LUN）またはCIFS共有は、SVMのボリューム内に作成され、Windowsホストおよびクラスタにマッピングされてストレージスペースを提供します（次の図を参照）。SVMはノードに依存せず、クラスタベースです。クラスタ内の任意の場所のボリュームやネットワークポートなどの物理リソースを使用できま

す。



Windows Server用のNetAppストレージのプロビジョニング

ストレージは、SAN環境とNAS環境の両方でWindows Serverにプロビジョニングできます。SAN環境では、ストレージはNetApp上のLUNのディスクとしてブロックストレージとして提供されます。NAS環境では、ストレージはファイルストレージとしてNetAppボリューム上のCIFS/SMB共有として提供されます。これらのディスクと共有は、次のようにWindows Serverに適用できます。

- アプリケーションワークロード用のWindows Serverホスト用ストレージ
- ナノサーバおよびコンテナ向けストレージ
- VMを格納するための個 々 のHyper-Vホストのストレージ
- VMを格納するCSV形式のHyper-Vクラスタ用共有ストレージ
- SQL Serverデータベース用のストレージ

NetAppストレージの管理

Windows Server 2016からNetAppストレージに接続、構成、および管理するには、次のいずれかの方法を使用します。

- セキュアシェル**(SSH)**。 Windows Server上の任意のSSHクライアントを使用して、NetApp CLIコマンドを実行します。
- * System Manager。*ネットアップのGUIベースの管理機能製品です。
- * NetApp PowerShell Toolkit。*これは、カスタムスクリプトおよびワークフローを自動化および実装するためのNetApp PowerShell Toolkitです。

NetApp PowerShellツールキット

NetApp PowerShell Toolkit（PSTK）は、NetApp ONTAPをエンドツーエンドで自動化し、ストレージ管理を可能にするPowerShellモジュールです。ONTAPモジュールには2、000を超えるコマンドレットが含まれており、FAS、NetApp All Flash FAS（AFF）、コモディティハードウェア、クラウドリソースの管理に役立ちます。

覚えておくべきこと

- NetAppでは、Windows Serverストレージスペースはサポートされていません。ストレージスペースはJBOD（単なるディスクの束）にのみ使用され、どのタイプのRAID（直接接続ストレージ[DAS]またはSAN）でも機能しません。
- Windows Serverのクラスタ化されたストレージプールは、ONTAPではサポートされていません。
- NetAppは、Windows SAN環境でのゲストクラスタリング用に共有仮想ハードディスクフォーマット（VHDX）をサポートしています。
- Windows Serverでは、iSCSI LUNまたはFC LUNを使用したストレージプールの作成はサポートされていません。

さらに読みます

- NetApp PowerShell Toolkitの詳細については、 "NetApp Support Site"。
- NetApp PowerShell Toolkitのベストプラクティスについては、を参照してください。 "TR-4475：『NetApp PowerShell Toolkit Best Practices Guide』"。

ネットワークのベストプラクティス

イーサネットネットワークは、次のグループに大きく分けることができます。

- VMのクライアントネットワーク
- 1つ以上のストレージネットワーク（ストレージシステムに接続するiSCSIまたはSMB）
- クラスタ通信ネットワーク（クラスタのノード間のハートビートおよびその他の通信）
- 管理ネットワーク（システムの監視とトラブルシューティング用）
- 移行ネットワーク（ホストのライブマイグレーション用）
- VMレプリケーション（Hyper-Vレプリカ）

ベストプラクティス

- NetAppでは、ネットワークの分離とパフォーマンスを確保するために、上記の機能ごとに専用の物理ポートを用意することを推奨しています。

- 上記のネットワーク要件（ストレージ要件を除く）ごとに、複数の物理ネットワークポートを集約して負荷を分散したり、フォールトトレランスを実現できます。
- NetAppでは、VM内のゲストストレージ接続用に、Hyper-Vホスト上に専用の仮想スイッチを作成することを推奨しています。
- Hyper-VホストとゲストiSCSIのデータパスで別 々 の物理ポートと仮想スイッチを使用して、ゲストとホスト間のセキュアな分離を実現します。
- NetAppでは、iSCSI NICのNICチーミングを避けることを推奨しています。
- NetAppでは、ストレージ用にホストに設定されたONTAP Multipath Input/Output（MPIO；マルチパス入出力）を使用することを推奨しています。
- ゲストiSCSIイニシエータを使用する場合は、ゲストVM内でMPIOを使用することを推奨しますNetApp。パススルーディスクを使用する場合は、ゲスト内でMPIOの使用を避ける必要があります。この場合、ホストにMPIOをインストールすれば十分です。
- NetAppでは、ストレージネットワークに割り当てられた仮想スイッチにQoSポリシーを適用しないことを推奨しています。
- NetAppでは、物理NICで自動プライベートIPアドレッシング（APIPA）を使用しないことを推奨しています。これは、APIPAがルーティングされず、DNSに登録されていないためです。
- NetAppでは、CSV、iSCSI、ライブマイグレーションの各ネットワークでジャンボフレームを有効にして、スループットを向上させ、CPUサイクルを短縮することを推奨しています。
- NetAppでは、Hyper-V仮想スイッチ用に管理オペレーティングシステムがこのネットワークアダプタを共有できるようにするオプションをオフにして、VM専用のネットワークを作成することを推奨しています。
- NetAppでは、ライブマイグレーション用に冗長なネットワークパス（複数のスイッチ）を作成し、耐障害性とQoSを確保することを推奨しています。

SAN環境でのプロビジョニング

ONTAP SVMは、ブロックプロトコルiSCSIおよびFCをサポートしています。ブロックプロトコルiSCSIまたはFCを使用してSVMを作成すると、SVMにはiSCSI Qualified Name（IQN）またはFC Worldwide Name（WWN）がそれぞれ取得されます。この識別子は、NetAppブロックストレージにアクセスするホストにSCSIターゲットを提供します。

Windows ServerでのNetApp LUNのプロビジョニング

前提条件

Windows ServerのSAN環境でNetAppストレージを使用するには、次の要件があります。

- NetAppクラスタには、1つ以上のNetAppストレージコントローラが設定されています。
- NetAppクラスタまたはストレージコントローラに有効なiSCSIライセンスがある。
- iSCSIポートまたはFCポートが設定されていることを確認します。
- FCゾーニングはFCスイッチでFC用に実行されます。
- アグリゲートが少なくとも1つ作成されている。

- SVMには、iSCSIまたはファイバチャネルを使用してデータを提供するすべてのストレージコントローラ上のイーサネットネットワークまたはファイバチャネルファブリックごとに1つのLIFが必要です。

導入

1. ブロックプロトコルiSCSIまたはFCを有効にして、新しいSVMを作成します。新しいSVMは次のいずれかの方法で作成できます。
   - NetAppストレージのCLIコマンド
   - ONTAP システムマネージャ
   - NetApp PowerShellツールキット
2. iSCSIプロトコル/ FCプロトコルを設定
3. SVMに各クラスタノードのLIFを割り当てます。
4. SVMでiSCSIサービス/ FCサービスを開始します。

   。
5. SVM LIFを使用して、iSCSIポートセットやFCポートセットを作成します。
6. 作成したポートセットを使用して、Windows用のiSCSIイニシエータ/ FCイニシエータグループを作成します。
7. イニシエータグループにイニシエータを追加します。イニシエータは、iSCSIのIQNとFCのWWPNです。Windows Serverからクエリを実行するには、PowerShellコマンドレットGet-InitiatorPortを実行します。

```
# Get the IQN for iSCSI
Get-InitiatorPort | Where \{$_.ConnectionType -eq 'iSCSI'} | Select-
Object -Property NodeAddress
```

```
# Get the WWPN for FC
Get-InitiatorPort | Where \{$_.ConnectionType -eq 'Fibre Channel'} |
Select-Object -Property PortAddress
```

```
# While adding initiator to the initiator group in case of FC, make sure
to provide the initiator(PortAddress) in the standard WWPN format
```

Windows Server上のiSCSIのIQNは、iSCSIイニシエータプロパティの構成でも確認できます。

- LUN作成ウィザードを使用してLUNを作成し、作成したイニシエータグループに関連付けます。

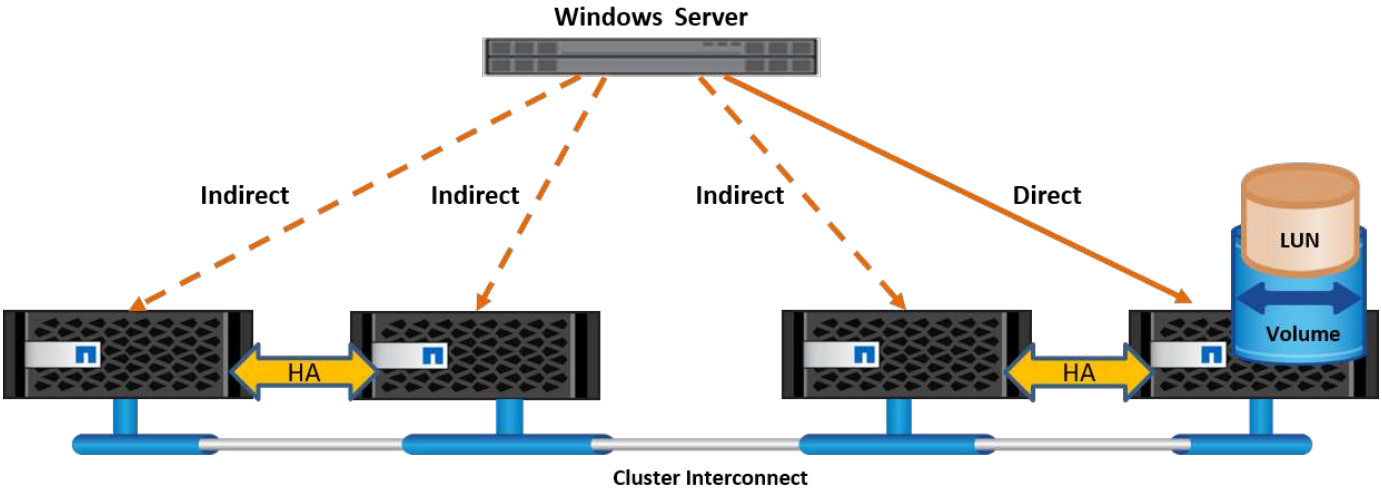
ホスト統合

Windows Serverでは、Asymmetrical Logical Unit Access（ALUA；非対称論理ユニットアクセス）拡張MPIOを使用して、LUNへの直接パスと間接パスを決定します。SVMが所有するすべてのLIFはLUNの読み取り/書き

込み要求を受け入れますが、そのLUNの元となるディスクを実際に所有しているクラスタノードは常に1つだけです。これにより、次の図に示すように、LUNへの使用可能なパスが直接パスと間接パスの2種類に分けられます。

LUNの直接パスとは、SVMのLIFとアクセス対象のLUNが同じノードにあるパスです。物理ターゲットポートからディスクに移動する場合、クラスタネットワークを経由する必要はありません。

間接パスは、SVMのLIFとアクセス対象のLUNが別 々 のノードにあるデータパスです。物理ターゲットポートからディスクに移動するには、データがクラスタネットワークを経由する必要があります。



MPIO

NetApp ONTAPは、ストレージコントローラからWindows Serverへの複数のパスが存在できる高可用性ストレージを提供します。マルチパスは、サーバからストレージアレイへの複数のデータパスを確立する機能です。マルチパスは、ハードウェア障害（ケーブルの切断、スイッチおよびHost Bus Adapter（HBA；ホストバスアダプタ）の障害など）から保護します。また、複数の接続を集約したパフォーマンスを使用することで、より高いパフォーマンス制限を実現できます。一方のパスまたは接続が使用できなくなると、マルチパスソフトウェアは自動的に他の使用可能なパスのいずれかに負荷を移します。MPIO機能は、ストレージへの複数の物理パスをデータアクセスに使用する単一の論理パスとして組み合わせて、ストレージの耐障害性と負荷分散を実現します。この機能を使用するには、Windows ServerでMPIO機能を有効にする必要があります。

MPIOを有効にする

Windows ServerでMPIOを有効にするには、次の手順を実行します。

1. 管理者グループのメンバーとしてWindows Serverにログインします。
2. Server Managerを起動します。
3. [管理]セクションで、[ロールと機能の追加]をクリックします。
4. [Select Features]ページで、[Multipath I/O]を選択します。

MPIOの設定

iSCSIプロトコルを使用する場合は、MPIOプロパティでiSCSIデバイスにマルチパスサポートを適用するようにWindows Serverに指示する必要があります。

Windows ServerでMPIOを設定するには、次の手順を実行します。

1. 管理者グループのメンバーとしてWindows Serverにログオンします。
2. Server Managerを起動します。
3. [ツール]セクションで、[MPIO]をクリックします。
4. [Discover Multi-Paths]の[MPIO Properties]で、[Add Support for iSCSI Devices]を選択し、[Add]をクリックします。コンピュータの再起動を求めるプロンプトが表示されます。
5. Windows Serverをリブートして、[MPIOのプロパティ]の[MPIOデバイス]セクションにMPIOデバイスが表示されることを確認します。

iSCSIを設定

Windows ServerでiSCSIブロックストレージを検出するには、次の手順を実行します。

1. 管理者グループのメンバーとしてWindows Serverにログオンします。
2. Server Managerを起動します。
3. [Tools]セクションで、[iSCSI Initiator]をクリックします。
4. [Discovery]タブで、[Discover Portal]をクリックします。
5. SANプロトコル用のNetAppストレージ用に作成したSVMに関連付けられているLIFのIPアドレスを指定します。[詳細設定]をクリックし、[全般]タブで情報を設定して、[OK]をクリックします。
6. iSCSIイニシエータによってiSCSIターゲットが自動的に検出され、[ターゲット]タブに一覧表示されます。
7. [Discovered Targets]でiSCSIターゲットを選択します。[Connect]をクリックして[Connect to Target]ウィンドウを開きます。
8. Windows ServerホストからNetAppストレージクラスタ上のターゲットiSCSI LIFへのセッションを複数作成する必要があります。これには、次の手順を実行します。
9. [Connect to Target]ウィンドウで、[Enable MPIO]を選択し、[Advanced]をクリックします。
10. [詳細設定]の[全般]タブで、ローカルアダプタをMicrosoft iSCSIイニシエータとして選択し、[イニシエータIP]と[ターゲットポータルIP]を選択します。
11. また、2番目のパスを使用して接続する必要があります。そのため、手順5から手順8を繰り返しますが、今回は2番目のパスとして[Initiator IP]と[Target Portal IP]を選択します。
12. [iSCSI Properties]メインウィンドウの[Discovered Targets]でiSCSIターゲットを選択し、[Properties]をクリックします。
13. [プロパティ]ウィンドウに、複数のセッションが検出されたことが表示されます。セッションを選択して[Devices]をクリックし、MPIOをクリックしてロードバランシングポリシーを設定します。デバイスに設定されているすべてのパスが表示され、すべてのロードバランシングポリシーがサポートされます。通常、NetAppではサブセットを使用したラウンドロビンを推奨しています。この設定は、ALUAが有効なアレイのデフォルトです。ラウンドロビンは、ALUAをサポートしないアクティブ/アクティブアレイのデフォルトです。

ブロックストレージを検出

Windows ServerでiSCSIまたはFCブロックストレージを検出するには、次の手順を実行します。

1. サーバーマネージャの[ツール]セクションで[コンピュータの管理]をクリックします。
2. [コンピュータの管理]で、[ストレージのディスクの管理]セクションをクリックし、[その他の操作]と[ディ

スクの再スキャン]をクリックします。これにより、raw iSCSI LUNが表示されます。

3. 検出されたLUNをクリックしてオンラインにします。次に、MBRまたはGPTパーティションを使用してディスクを初期化を選択します。ボリュームサイズとドライブ文字を指定して新しいシンプルボリュームを作成し、FAT、FAT32、NTFS、またはResilient File System（ReFS）を使用してフォーマットします。

ベストプラクティス

- NetAppでは、LUNをホストするボリュームでシンプロビジョニングを有効にすることを推奨しています。
- マルチパスの問題を回避するために、NetAppでは、特定のLUNに対するすべての10Gbセッションまたはすべての1Gbセッションのいずれかを使用することを推奨しています。
- NetAppでは、ストレージシステムでALUAが有効になっていることを確認することを推奨しています。ONTAPでは、ALUAがデフォルトで有効になっています。
- NetApp LUNのマッピング先のWindows Serverホストで、ファイアウォールの設定で、インバウンドの場合はiSCSIサービス（TCP-IN）、アウトバウンドの場合はiSCSIサービス（TCP-OUT）を有効にします。これらの設定により、Hyper-VホストおよびNetAppコントローラとの間でiSCSIトラフィックが送受信されます。

NanoサーバでのNetApp LUNのプロビジョニング

前提条件

前のセクションで説明した前提条件に加えて、ストレージロールをNano Server側から有効にする必要があります。たとえば、Nano Serverは-Storageオプションを使用して導入する必要があります。Nano Serverを展開するには、「"Nano Serverを展開します。""

導入

ナノサーバでNetApp LUNをプロビジョニングするには、次の手順を実行します。

1. 「"Nanoサーバーへの接続". 」
2. iSCSIを設定するには、Nano Serverで次のPowerShellコマンドレットを実行します。

```
# Start iSCSI service, if it is not already running
Start-Service msiscsi
```

```
# Create a new iSCSI target portal
New-IscsiTargetPortal â€"TargetPortalAddress <SVM LIF>
```

```
# View the available iSCSI targets and their node address
Get-IscsiTarget
```

```
# Connect to iSCSI target
Connect-IscsiTarget -NodeAddress <NodeAddress>
```

```
# NodeAddress is retrived in above cmdlet Get-IscsiTarget
# OR
Get-IscsiTarget | Connect-IscsiTarget
```

```
# View the established iSCSI session
Get-IscsiSession
```

```
# Note the InitiatorNodeAddress retrieved in the above cmdlet Get-
IscsiSession. This is the IQN for Nano server and this needs to be added
in the Initiator group on NetApp Storage
```

```
# Rescan the disks
Update-HostStorageCache
```

3. イニシエータグループにイニシエータを追加します。

```
Add the InitiatorNodeAddress retrieved from the cmdlet Get-IscsiSession
to the Initiator Group on NetApp Controller
```

4. MPIOを設定します。

```
# Enable MPIO Feature
Enable-WindowsOptionalFeature -Online -FeatureName MultipathIo
```

```
# Get the Network adapters and their IPs
Get-NetIPAddress â€"AddressFamily IPv4 â€"PrefixOrigin <Dhcp or Manual>
```

```
# Create one MPIO-enabled iSCSI connection per network adapter
Connect-IscsiTarget -NodeAddress <NodeAddress> -IsPersistent $True â
€"IsMultipathEnabled $True â€"InitiatorPortalAddress <IP Address of
ethernet adapter>
```

```
# NodeAddress is retrieved from the cmdlet Get-IscsiTarget
# IPs are retrieved in above cmdlet Get-NetIPAddress
```

```
# View the connections
Get-IscsiConnection
```

5. ブロックストレージを検出

```
# Rescan disks
Update-HostStorageCache
```

```
# Get details of disks
Get-Disk
```

```
# Initialize disk
Initialize-Disk -Number <DiskNumber> -PartitionStyle <GPT or MBR>
```

```
# DiskNumber is retrived in the above cmdlet Get-Disk
# Bring the disk online
Set-Disk -Number <DiskNumber> -IsOffline $false
```

```
# Create a volume with maximum size and default drive letter
New-Partition -DiskNumber <DiskNumber> -UseMaximumSize
-AssignDriveLetter
```

```
# To choose the size and drive letter use -Size and -DriveLetter
parameters
# Format the volume
Format-Volume -DriveLetter <DriveLetter> -FileSystem <FAT32 or NTFS or
REFS>
```

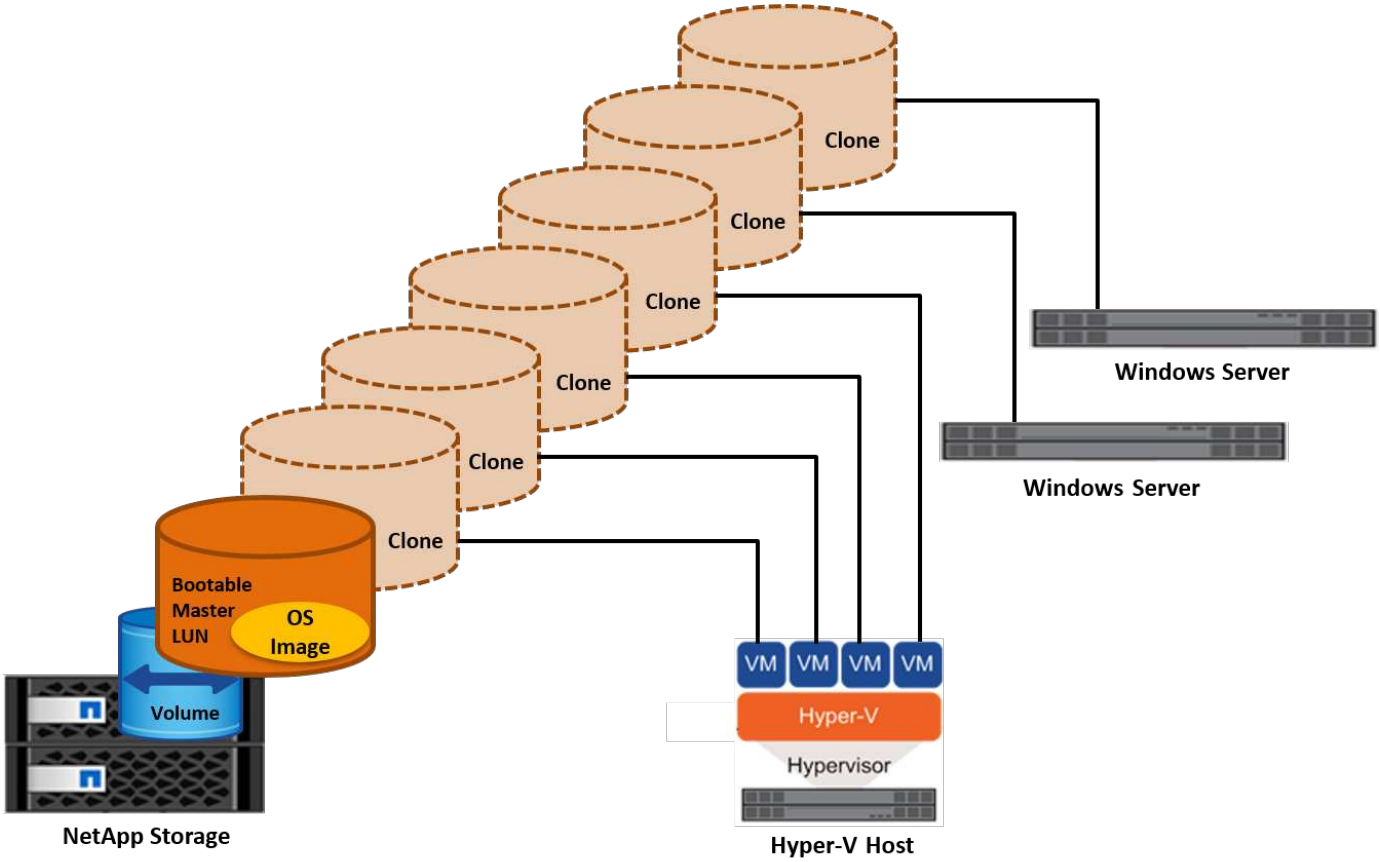
SANからのブート

物理ホスト（サーバ）またはHyper-V VMは、内蔵ハードディスクではなくNetApp LUNから直接Windows Server OSをブートできます。SANブートのアプローチでは、ブート元のOSイメージは、物理ホストまたはVMに接続されたNetApp LUNに格納されます。物理ホストの場合、物理ホストのHBAは、NetApp LUNをブ

ートに使用するように設定されます。VMの場合、NetApp LUNはブート用のパススルーディスクとして接続されます。

NetApp FlexCloneのアプローチ

NetApp FlexCloneテクノロジを使用すると、次の図に示すように、OSイメージを含むブートLUNのクローンを瞬時に作成し、サーバやVMに接続して、クリーンなOSイメージを迅速に提供できます。



物理ホストのSANからのブート

前提条件

- 物理ホスト（サーバ）に適切なiSCSI HBAまたはFC HBAが搭載されている。
- Windows Serverをサポートしているサーバに適したHBAデバイスドライバをダウンロードしておきます。
- サーバーにWindows Server ISOイメージを挿入するのに適したCD/DVDドライブまたは仮想メディアがあり、HBAデバイスドライバがダウンロードされている。
- NetApp iSCSIまたはFC LUNは、NetAppストレージコントローラ上にプロビジョニングされます。

導入

物理ホストに対してSANからのブートを設定するには、次の手順を実行します。

1. サーバHBAでBootBIOSを有効にします
2. iSCSI HBAの場合は、ブートBIOS設定でイニシエータIP、iSCSIノード名、およびアダプタのブートモードを設定します。

3. NetAppストレージコントローラでiSCSIまたはFCのイニシエータグループを作成する場合は、サーバHBAイニシエータをグループに追加します。サーバのHBAイニシエータは、FC HBAのWWPNまたはiSCSI HBAのiSCSIノード名です。
4. NetAppストレージコントローラにLUN ID 0のLUNを作成し、前の手順で作成したイニシエータグループに関連付けます。このLUNはブートLUNとして機能します。
5. HBAをブートLUNへの単一のパスに制限します。Windows ServerをブートLUNにインストールしたあとにパスを追加して、マルチパス機能を利用できます。
6. HBAのBootBIOSユーティリティを使用して、LUNをブートデバイスとして設定します。
7. ホストをリブートし、ホストBIOSユーティリティを起動します。
8. ブートLUNがブート順序の最初のデバイスになるようにホストBIOSを設定します。
9. Windows Server ISOから、インストールセットアップを起動します。
10. 「Where do you want to install Windows？」というメッセージが表示されたら、インストール画面の下部にある「Load Driver（ドライバのロード）」をクリックして、「Select Driver to Install（インストールするドライバの選択）」ページを起動します。前の手順でダウンロードしたHBAデバイスドライバのパスを入力し、ドライバのインストールを完了します。
11. これで、前の手順で作成したブートLUNがWindowsのインストールページに表示されるようになります。ブートLUNにWindows Serverをインストールするブート LUNを選択し、インストールを完了します。

仮想マシンの**SAN**からのブート

VMに対してSANからのブートを設定するには、次の手順を実行します。

導入

1. NetAppストレージコントローラでiSCSIまたはFCのイニシエータグループを作成する場合は、Hyper-VサーバのIQN（iSCSIの場合）またはWWN（FCの場合）をコントローラに追加します。
2. NetAppストレージコントローラでLUNまたはLUNクローンを作成し、前の手順で作成したイニシエータグループに関連付けます。これらのLUNは、VMのブートLUNとして機能します。
3. Hyper-Vサーバ上のLUNを検出してオンラインにし、初期化します。
4. LUNをオフラインにします。
5. [Connect Virtual Hard Disk]ページで、[Attach a Virtual Hard Disk]オプションを使用してVMを作成します。
6. LUNをVMにパススルーディスクとして追加します。
   a. VM設定を開きます。
   b. [IDE Controller 0]をクリックし、[Hard Drive]を選択して、[Add]をクリックします。[IDE Controller 0]を選択すると、このディスクがVMの最初の起動デバイスになります。
   c. [Hard Disk]オプションで[Physical Hard Disk]を選択し、リストからパススルーディスクとしてディスクを選択します。ディスクは、前の手順で設定したLUNです。
7. パススルーディスクにWindows Serverをインストールします。

ベストプラクティス

- LUNがオフラインであることを確認します。そうしないと、ディスクをVMにパススルーディスクとして追加できません。

- LUNが複数存在する場合は、ディスク管理でLUNのディスク番号をメモしておいてください。VMのリストにはディスク番号が記載されているため、この処理は必須です。また、VMのパススルーディスクとしてのディスクの選択は、このディスク番号に基づいて行われます。
- NetAppでは、iSCSI NICのNICチーミングを避けることを推奨しています。
- NetAppでは、ストレージ用にホストに設定されたONTAP MPIOを使用することを推奨しています。

SMB環境でのプロビジョニング

ONTAPは、SMB3プロトコルを使用して、Hyper-V仮想マシン用に耐障害性とパフォーマンスに優れたNASストレージを提供します。

CIFSプロトコルを使用してSVMを作成すると、Windows Active Directoryドメインに属するSVM上でCIFSサーバが実行されます。SMB共有をホームディレクトリに使用したり、Hyper-VおよびSQL Serverのワークロードをホストしたりできます。ONTAPでは、SMB 3.0の次の機能がサポートされます。

- 永続的ハンドル（継続的可用性を備えたファイル共有）
- カンシフロトコル
- クラスタクライアントフェイルオーバー
- スケールアウト対応
- ODX
- リモオトVSS

Windows ServerでのSMB共有のプロビジョニング

前提条件

Windows ServerのNAS環境でNetAppストレージを使用するには、次の要件があります。

- ONTAPクラスタに有効なCIFSライセンスが必要です。
- アグリゲートが少なくとも1つ作成されている。
- データ論理インターフェイス（LIF）が1つ作成され、そのデータLIFをCIFS用に設定する必要があります。
- DNSが設定したWindows Active Directoryドメインサーバとドメイン管理者のクレデンシャルがある。
- NetAppクラスタ内の各ノードは、Windowsドメインコントローラと時刻が同期されます。

Active Directoryドメインコントローラ

NetAppストレージコントローラは、Windowsサーバと同様にActive Directoryに参加して、Active Directory内で動作することができます。SVMの作成時に、ドメイン名とネームサーバの詳細を指定してDNSを設定できます。SVMは、Windows Serverと同様の方法で、DNSにActive Directory / Lightweight Directory Access Protocol（LDAP）サーバを照会することで、Active Directoryドメインコントローラの検索を試みます。

CIFSのセットアップが正しく機能するためには、NetAppストレージコントローラとWindowsドメインコントローラの時刻が同期されている必要があります。NetAppでは、WindowsドメインコントローラとNetAppストレージコントローラの間の時間差を5分以内にすることを推奨しています。ONTAPクラスタを外部の時間ソー

スと同期するには、ネットワークタイムプロトコル（NTP）サーバを設定することを推奨します。Windowsドメインコントローラを NTPサーバとして設定するには、ONTAPクラスタで次のコマンドを実行します。

```
$domainControllerIP = "<input IP Address of windows domain controller>"
cluster::> system services ntp server create â€"server $domainControllerIP
```

導入

1. 新しいSVMを作成してNASプロトコルCIFSを有効にします。新しいSVMは次のいずれかの方法で作成できます。
   - NetApp ONTAPノCLIコマント
   - System Manager の略
   - NetApp PowerShellツールキット
2. CIFSプロトコルの設定
   a. CIFSサーバ名を指定します。
   b. CIFSサーバを追加するActive Directoryを指定します。CIFSサーバをActive Directoryに追加するには、ドメイン管理者のクレデンシャルが必要です。
3. SVMに各クラスタノードのLIFを割り当てます。
4. SVMでCIFSサービスを開始します。
5. アグリゲートからNTFSセキュリティ形式のボリュームを作成します。
6. ボリュームにqtreeを作成します（オプション）。
7. Windows Serverからアクセスできるように、ボリュームまたはqtreeディレクトリに対応する共有を作成します。共有をHyper-Vストレージに使用する場合は、共有の作成時にHyper-Vの継続的可用性を有効にするを選択します。これにより、ファイル共有の高可用性が実現します。
8. 作成した共有を編集し、共有へのアクセスに必要に応じて権限を変更します。SMB共有にアクセスするすべてのサーバのコンピュータアカウントにアクセスを許可するように、SMB共有の権限を設定する必要があります。

ホスト統合

NASプロトコルCIFSは、ONTAPに標準で統合されています。したがって、Windows Serverは、NetApp ONTAP上のデータにアクセスするために追加のクライアントソフトウェアを必要としません。NetAppストレージコントローラは、ネットワーク上でネイティブファイルサーバとして認識され、Microsoft Active Directory認証をサポートします。

Windows Serverで作成したCIFS共有を検出するには、次の手順を実行します。

1. 管理者グループのメンバーとしてWindows Serverにログインします。
2. run.exeに移動し、共有にアクセスするために作成したCIFS共有の完全パスを入力します。
3. 共有をWindows Serverに永続的にマッピングするには、[This PC]を右クリックし、[Map Network Drive]をクリックして、CIFS共有のパスを指定します。
4. 一部のCIFS管理タスクは、Microsoft管理コンソール（MMC）を使用して実行できます。これらのタスクを実行する前に、MMCメニューコマンドを使用してMMCをNetApp ONTAPストレージに接続する必要が

あります。

a. Windows ServerでMMCを開くには、サーバーマネージャの[ツール]セクションで[コンピュータの管理]をクリックします。

b. [その他の操作]をクリックして[別のコンピュータに接続]をクリックすると、[コンピュータの選択]ダイアログが開きます。

c. CIFSサーバの名前またはCIFSサーバに接続するSVM LIFのIPアドレスを入力します。

d. [システムツール]と[共有フォルダ]を展開して、開いているファイル、セッション、および共有を表示および管理します。

ベストプラクティス

- NetAppでは、ボリュームがあるノードから別のノードに移動されたときやノードで障害が発生したときにダウンタイムが発生しないことを確認するために、ファイル共有でcontinuous availabilityオプションを有効にすることを推奨しています。
- Hyper-V over SMB環境用にVMをプロビジョニングする場合はNetApp、ストレージシステムでコピーオフロードを有効にすることを推奨します。これにより、VMのプロビジョニング時間が短縮されます。
- ストレージクラスタでSQL Server、Hyper-V、CIFSサーバなどの複数のSMBワークロードをホストするNetApp場合は、別 々 のアグリゲートにある別 々 のSVMで異なるSMBワークロードをホストすることを推奨します。この構成は、各ワークロードに固有のストレージネットワークとボリュームレイアウトが必要になるため、有益です。
- NetAppでは、Hyper-VホストとNetApp ONTAPストレージを10GBのネットワーク（使用可能な場合）で接続することを推奨しています。1GBのネットワーク接続の場合、NetAppでは、複数の1GBポートで構成されるインターフェイスグループを作成することを推奨します。
- NetAppでは、あるSMB 3.0共有から別の共有にVMを移行する際に、移行時間を短縮するために、ストレージシステムでCIFSコピーオフロード機能を有効にすることを推奨しています。

覚えておくべきこと

- SMB環境用のボリュームをプロビジョニングする場合は、ボリュームをNTFSセキュリティ形式で作成する必要があります。
- クラスタ内のノードの時間設定は、それに応じて設定する必要があります。NetApp CIFSサーバがWindows Active Directoryドメインに参加している必要がある場合は、NTPを使用します。
- 永続的ハンドルは、HAペアのノード間でのみ機能します。
- 監視プロトコルは、HAペアのノード間でのみ機能します。
- 継続的可用性を備えたファイル共有は、Hyper-VおよびSQL Serverワークロードでのみサポートされます。
- SMBマルチチャネルはONTAP 9.4以降でサポートされます。
- RDMAはサポートされません。
- Refsはサポートされていません。

Nanoサーバーでの**SMB**共有のプロビジョニング

Nano Serverでは、NetAppストレージコントローラ上のCIFS共有上のデータにアクセスするために、追加のクライアントソフトウェアは必要ありません。

Nano ServerからCIFS共有にファイルをコピーするには、リモートサーバで次のコマンドレットを実行します。

```
$ip = "<input IP Address of the Nano Server>"
```

```
# Create a New PS Session to the Nano Server
$session = New-PSSession -ComputerName $ip -Credential ~\Administrator
```

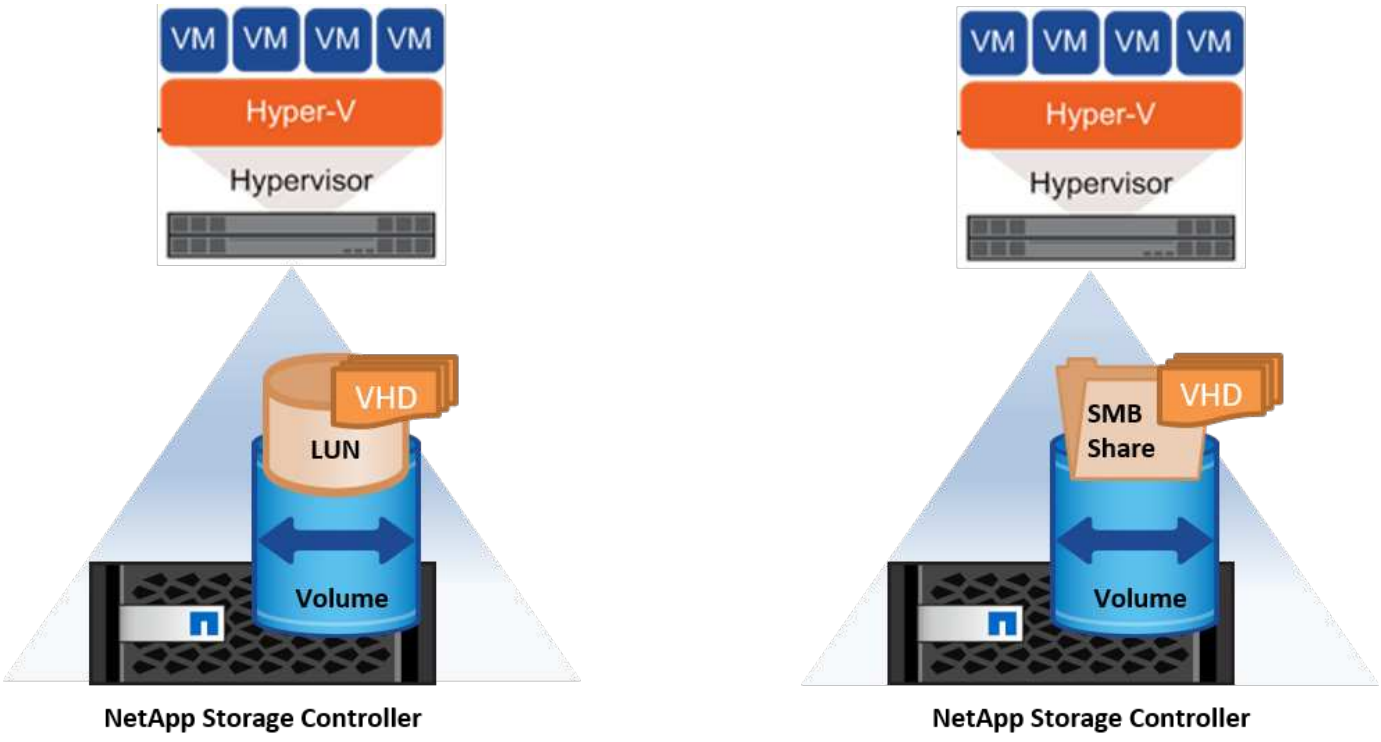
```
 Copy-Item -FromSession $s -Path C:\Windows\Logs\DISM\dism.log
-Destination \\cifsshare
* `cifsshare` は、NetAppストレージコントローラ上のCIFS共有です。
* Nano Serverにファイルをコピーするには、次のコマンドレットを実行します。
```

+
Copy-Item -ToSession $s -Path \\cifsshare\<file> -Destination C:\

フォルダの内容全体をコピーするには、フォルダ名を指定し、コマンドレットの末尾にある-Recurseパラメータを使用します。

NetApp上のHyper-Vストレージインフラ

Hyper-Vストレージインフラは、ONTAPストレージシステムでホストできます。Hyper-VでVMファイルとそのディスクを格納するためのストレージは、次の図に示すように、NetApp LUNまたはNetApp CIFS共有を使用して提供できます。



NetApp LUN上のHyper-Vストレージ

- Hyper-VサーバマシンでNetApp LUNをプロビジョニングします。詳細については、「"SAN環境でのプロビジョニング". 」
- [Server Manager]の[Tools]セクションから[Hyper-V Manager]を開きます。
- Hyper-Vサーバを選択し、[Hyper-V Settings]をクリックします。
- VMとそのディスクをLUNとして格納するデフォルトのフォルダを指定します。これにより、Hyper-Vストレージのデフォルトパスが LUNとして設定されます。VMのパスを明示的に指定する場合は、VMの作成時に指定できます。

NetApp CIFS上のHyper-Vストレージ

このセクションに記載されている手順を開始する前に、"SMB環境でのプロビジョニング"」。 NetApp CIFS共有でHyper-Vストレージを設定するには、次の手順を実行します。

1. [Server Manager]の[Tools]セクションから[Hyper-V Manager]を開きます。
2. Hyper-Vサーバを選択し、[Hyper-V Settings]をクリックします。
3. VMとそのディスクをCIFS共有として格納するデフォルトのフォルダを指定します。これにより、Hyper-VストレージのCIFS共有としてデフォルトパスが設定されます。VMのパスを明示的に指定する場合は、VMの作成時に指定できます。

Hyper-Vの各VMには、物理ホストに提供されたNetApp LUNとCIFS共有を提供できます。この手順は、任意の物理ホストの場合と同じです。VMにストレージをプロビジョニングするには、次の方法を使用します。

- VM内のFCイニシエータを使用したストレージLUNの追加
- VM内のiSCSIイニシエータを使用したストレージLUNの追加
- VMへのパススルー物理ディスクの追加
- ホストからVMへのVHD / VHDXの追加

ベストプラクティス

- VMとそのデータがNetAppストレージに格納される場合、NetAppでは、NetApp重複排除をボリュームレベルで定期的に実行することを推奨しています。これにより、同一のVMがCSV共有またはSMB共有でホストされている場合、スペースが大幅に削減されます。重複排除はストレージコントローラ上で実行され、ホストシステムとVMのパフォーマンスには影響しません。
- Hyper-VでiSCSI LUNを使用する場合は、 `iSCSI Service (TCP-In) for Inbound` および `iSCSI Service (TCP-Out) for Outbound` Hyper-Vホストのファイアウォール設定。これにより、Hyper-VホストとNetAppコントローラとの間でiSCSIトラフィックが送受信されます。
- NetAppでは、[Allow Management Operating System to Share this Network Adapter for the Hyper-V virtual switch]オプションをオフにすることを推奨しています。これにより、VM専用のネットワークが作成されます。

覚えておくべきこと

- 仮想ファイバチャネルを使用してVMをプロビジョニングするには、NポートID仮想化が有効なFC HBAが必要です。最大4つのFCポートがサポートされます。

- ホストシステムに複数のFCポートが設定されており、VMに提供されている場合は、マルチパスを有効にするためにMPIOをVMにインストールする必要があります。
- パススルーディスクではMPIOがサポートされないため、そのホストでMPIOが使用されている場合、パススルーディスクをホストにプロビジョニングすることはできません。
- VHD / VHDxファイルに使用するディスクは、割り当てに64Kのフォーマットを使用する必要があります。

さらに読みます

- FC HBAの詳細については、を参照してください。 "NetApp Interoperability Matrix を参照してください"。
- 仮想ファイバチャネルの詳細については、Microsoftの "Hyper-V仮想ファイバチャネルの概要" ページ

オフロードデータ転送

Microsoft ODX（コピーオフロード）を使用すると、ホストコンピュータを介さずに、ストレージデバイス内または互換性があるストレージデバイス間でデータを直接転送できます。NetApp ONTAPは、CIFSプロトコルとSANプロトコルの両方でODX機能をサポートしています。ODXを使用すると、コピーが同じボリューム内にある場合にパフォーマンスが向上したり、クライアントでのCPUとメモリの使用率が低下したり、ネットワークI/O帯域幅の使用率が低下したりする可能性があります。

ODXを使用すると、SMB共有内、LUN内、およびSMB共有とLUN（同じボリューム内の場合）間でファイルをコピーする処理が高速かつ効率的になります。この方法は、OS（VHD / VHDX）のゴールデンイメージの複数のコピーが同じボリューム内に必要な場合に役立ちます。コピーが同じボリューム内にある場合、同じゴールデンイメージの複数のコピーを作成する時間が大幅に短縮されます。ODXは、VMストレージを移動するためのHyper-Vストレージのライブマイグレーションでも適用されます。

複数のボリューム間でコピーを行う場合は、ホストベースのコピーに比べてパフォーマンスが大幅に向上することはありません。

CIFSでODX機能を有効にするには、NetAppストレージコントローラで次のCLIコマンドを実行します。

1. CIFS用のODXを有効にします。
   #権限レベルをdiagnosticに設定する
   cluster：：> set -privilege diagnostic

   ```
   #enable the odx feature
   cluster::> vserver cifs options modify -vserver <vserver_name> -copy
   -offload-enabled true
   ```

   ```
   #return to admin privilege level
   cluster::> set privilege admin
   ```

2. SANでODX機能を有効にするには、NetAppストレージコントローラで次のCLIコマンドを実行します。
   #権限レベルをdiagnosticに設定する
   cluster：：> set -privilege diagnostic

```
#enable the odx feature
cluster::> copy-offload modify -vserver <vserver_name> -scsi enabled
```

```
#return to admin privilege level
cluster::> set privilege admin
```

覚えておくべきこと

- CIFSの場合、ODXを使用できるのは、クライアントとストレージサーバの両方でSMB 3.0およびODX機能がサポートされている場合だけです。
- SAN環境でODXを使用できるのは、クライアントとストレージサーバの両方でODX機能がサポートされている場合のみです。

さらに読みます

ODXの詳細については、を参照してください。 "Microsoftリモートコピーのパフォーマンスの向上" および "Microsoftオフロードデータ転送" 。

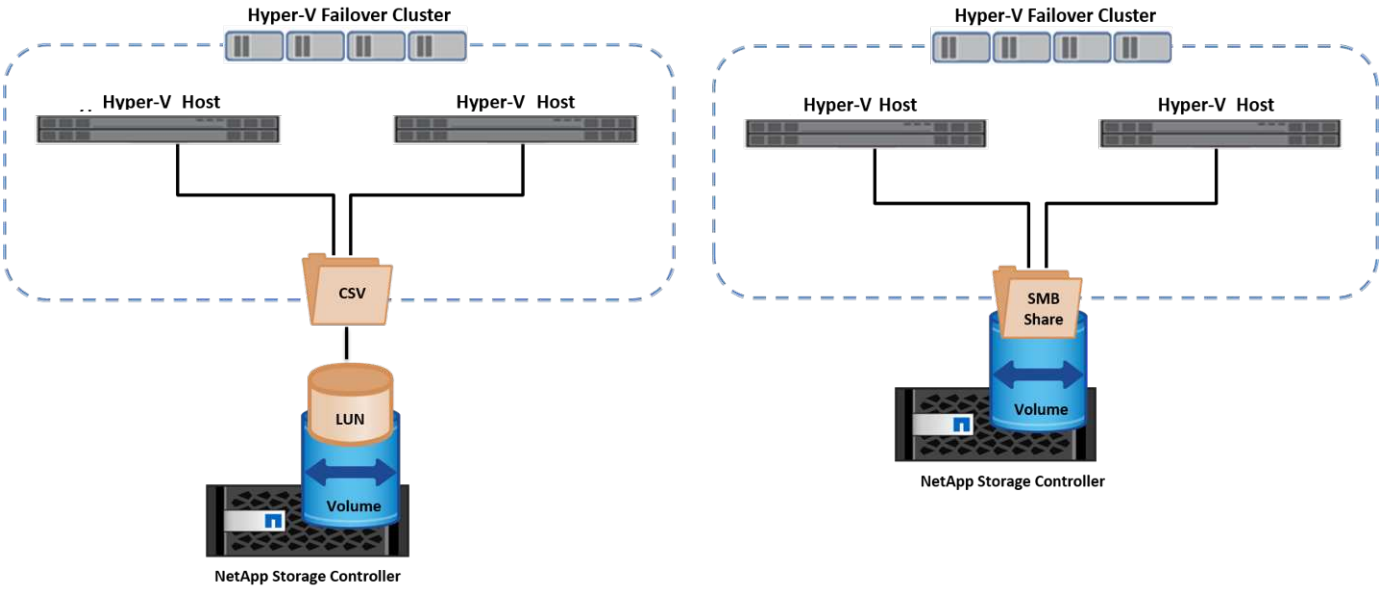
Hyper-Vクラスタリング：仮想マシンの高可用性と拡張性

フェイルオーバークラスタは、Hyper-Vサーバに対して高可用性と拡張性を提供します。フェイルオーバークラスタは、VMの可用性と拡張性を高めるために連携する独立したHyper-Vサーバのグループです。

Hyper-Vクラスタサーバ（ノード）は、物理ネットワークとクラスタソフトウェアによって接続されます。これらのノードは共有ストレージを使用して、構成、仮想ハードディスク（VHD）ファイル、Snapshotコピーなどの VMファイルを格納します。共有ストレージには、図6に示すように、NetApp SMB/CIFS共有またはNetApp LUN上のCSVを使用できます。この共有ストレージは、一貫性のある分散されたネームスペースを提供し、クラスタ内のすべてのノードから同時にアクセスできます。したがって、クラスタ内の1つのノードに障害が発生すると、もう一方のノードがフェイルオーバーと呼ばれるプロセスによってサービスを提供します。フェイルオーバークラスタは、フェイルオーバークラスタマネージャスナップインおよびフェイルオーバークラスタリングWindows PowerShellコマンドレットを使用して管理できます。

クラスタ共有ボリューム

CSVを使用すると、NTFSまたはReFSボリュームとしてプロビジョニングされた同じNetApp LUNへの読み取り/書き込みアクセスを、フェイルオーバークラスタ内の複数のノードで同時に実行できます。CSVを使用すると、クラスタ化されたロールは、ドライブ所有権を変更したり、ボリュームをディスマウントおよび再マウントしたりすることなく、ノード間で迅速にフェイルオーバーできます。CSVを使用すると、フェイルオーバークラスタ内の多数のLUNを簡単に管理できます。CSVは、NTFSまたはReFS上に階層化された汎用クラスタファイルシステムを提供します。



ベストプラクティス

- NetAppでは、内部クラスタ通信とCSVトラフィックが同じネットワークを経由しないように、iSCSIネットワークでクラスタ通信をオフにすることを推奨しています。
- NetAppでは、耐障害性とQoSを確保するために冗長なネットワークパス（複数のスイッチ）を使用することを推奨しています

覚えておくべきこと

- CSVに使用するディスクは、NTFSまたはReFSでパーティショニングする必要があります。FATまたはFAT32でフォーマットされたディスクはCSVに使用できません。
- CSVに使用するディスクの割り当てには64Kのフォーマットを使用する必要があります。

さらに読みます

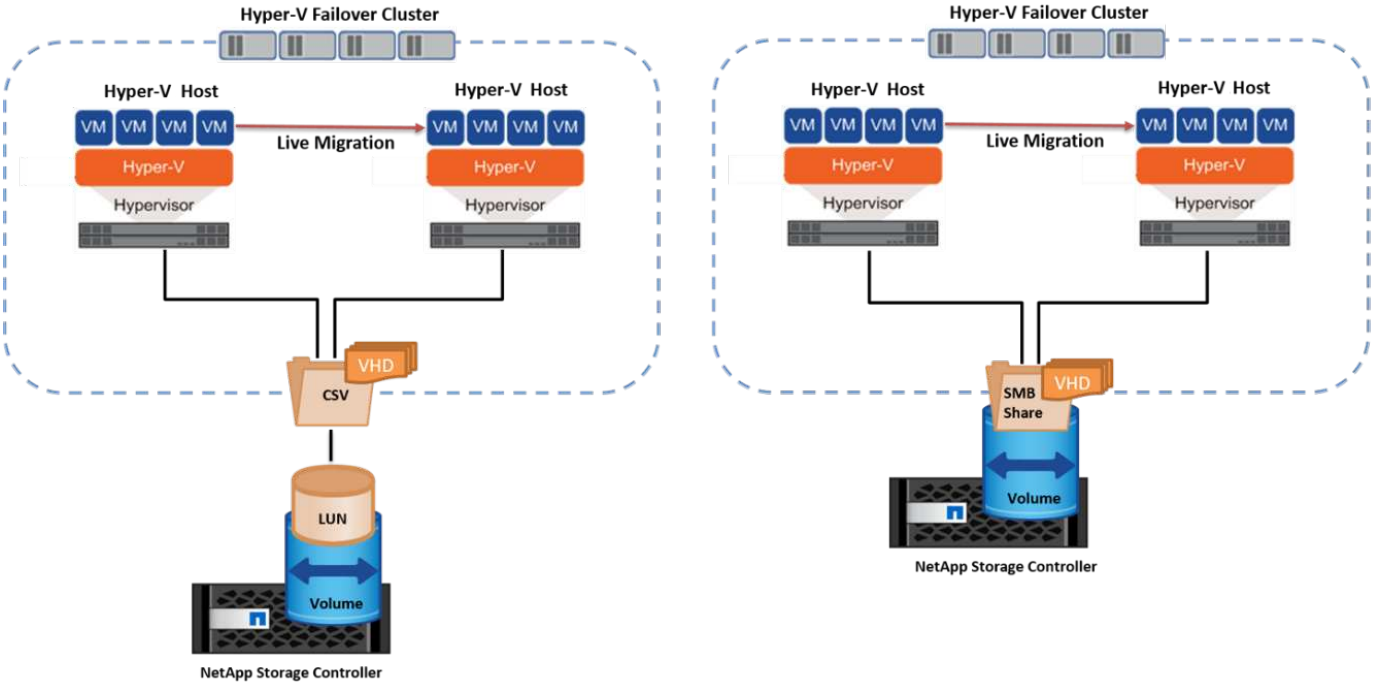
Hyper-Vクラスタの導入については、「付録B： "Hyper-Vクラスタの導入"。

Hyper-Vライブマイグレーション：VMの移行

VMの有効期間中に、Windowsクラスタ上の別のホストにVMを移動しなければならない場合があります。この処理は、ホストのシステムリソースが不足している場合や、メンテナンスのためにホストのリブートが必要な場合に必要になることがあります。同様に、VMを別のLUNまたはSMB共有に移動しなければならない場合があります。これは、現在のLUNまたは共有でスペースが不足しているか、パフォーマンスが想定よりも低い場合に必要になることがあります。Hyper-Vライブマイグレーションでは、実行中のVMを物理Hyper-Vサーバ間で移動します。VMの可用性には影響しません。フェイルオーバークラスタの一部であるHyper-Vサーバ間、またはどのクラスタにも属さない独立したHyper-Vサーバ間で、VMをライブマイグレーションできます。

クラスタ環境でのライブマイグレーション

VMは、クラスタのノード間でシームレスに移動できます。クラスタ内のすべてのノードが同じストレージを共有し、VMとそのディスクにアクセスできるため、VMの移行は瞬時に完了します。次の図に、クラスタ環境でのライブマイグレーションを示します。



ベストプラクティス

- ライブマイグレーショントラフィック専用のポートを用意します。
- 移行中のネットワーク関連の問題を回避するために、専用のホストライブマイグレーションネットワークを用意します。

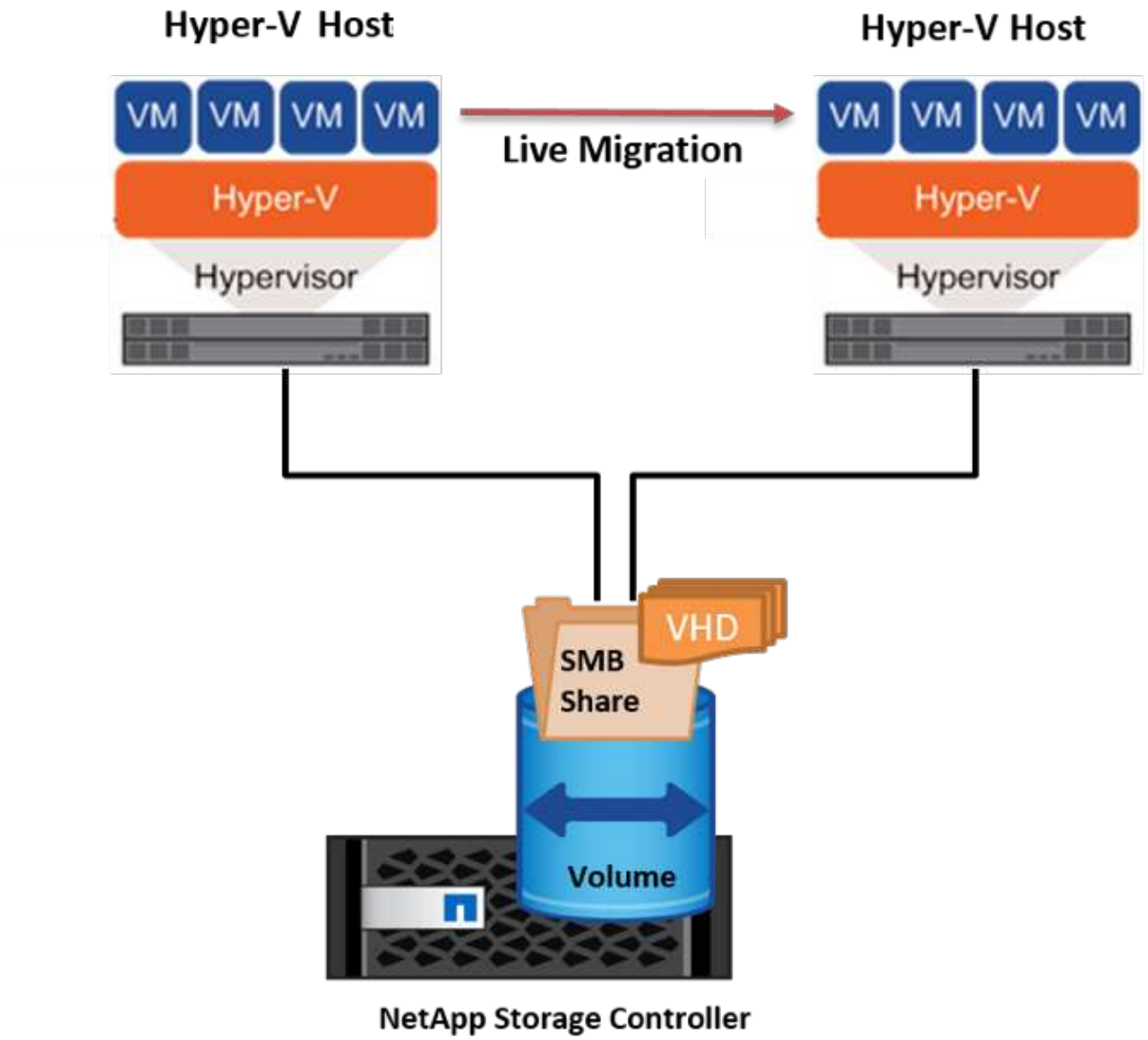
さらに読みます

クラスタ環境へのライブマイグレーションの導入については、を参照してください。 "付録C：クラスタ環境へのHyper-Vライブマイグレーションの導入"。

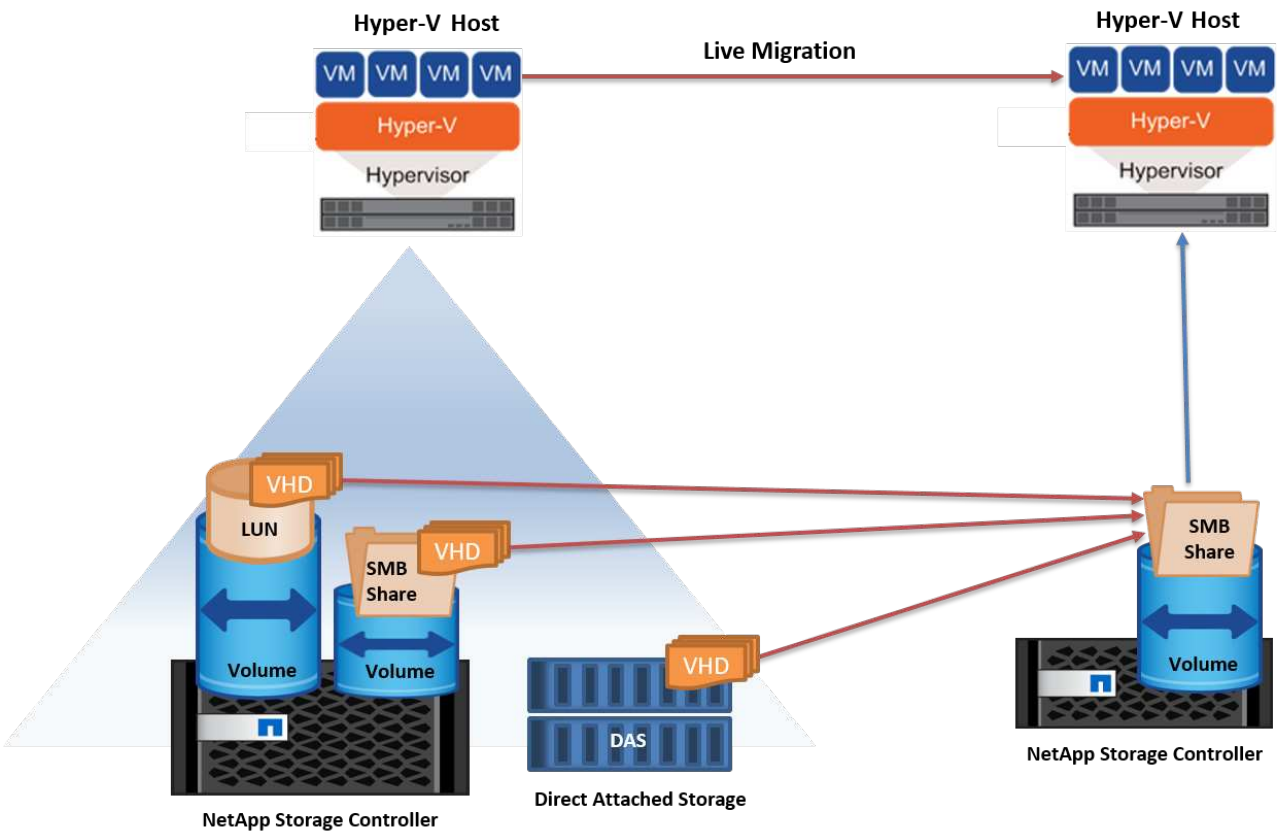
クラスタ環境外でのライブマイグレーション

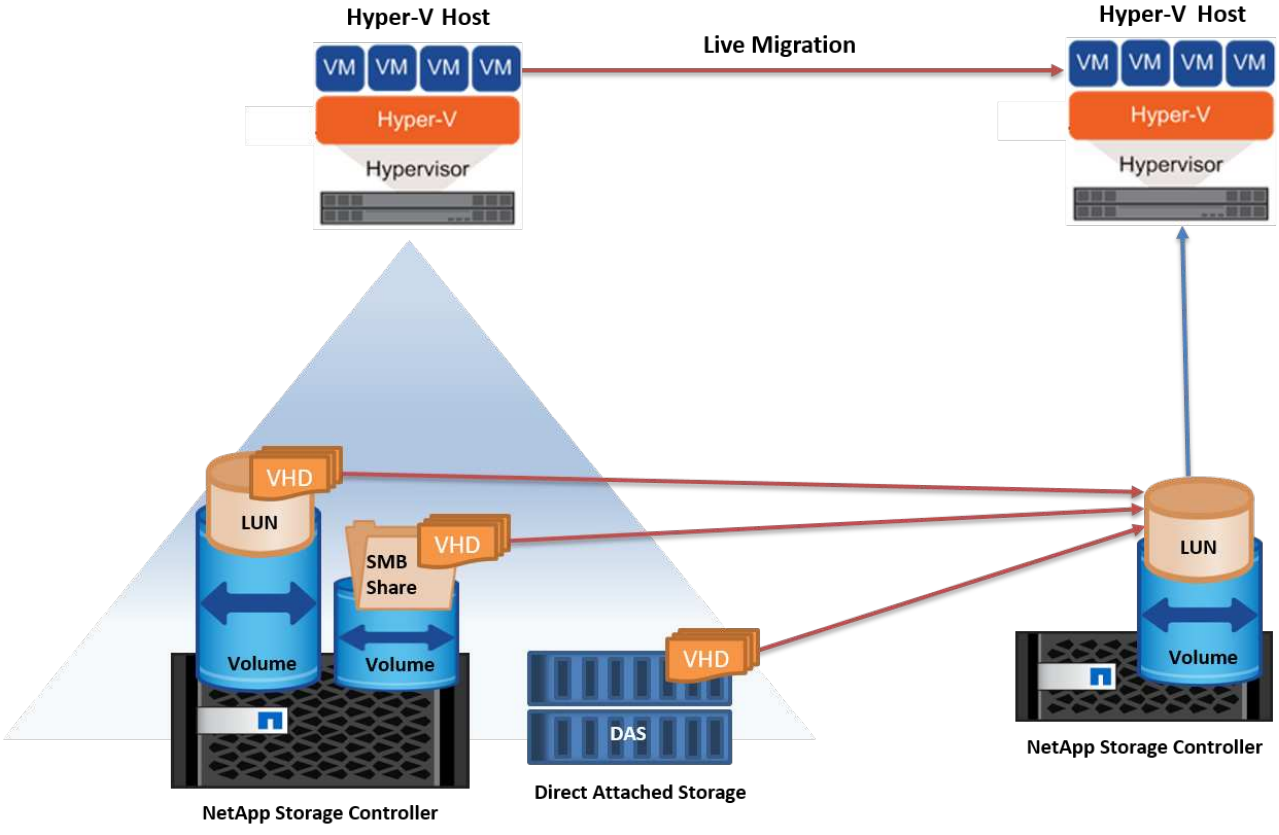
VMは、クラスタ化されておらず、独立した2台のHyper-Vサーバ間でライブマイグレーションできます。このプロセスでは、シェアードナッシングまたはシェアードナッシングライブマイグレーションを使用できます。

- 共有ライブマイグレーションでは、VMはSMB共有に格納されます。したがって、VMをライブマイグレーションする場合、次の図に示すように、VMのストレージは中央のSMB共有に残り、もう一方のノードから即座にアクセスできます。



- シェアードナッシングライブマイグレーションでは、各Hyper-Vサーバに独自のローカルストレージ（SMB共有、LUN、DAS）があり、VMのストレージはHyper-Vサーバに対してローカルになります。VMをライブマイグレーションすると、VMのストレージがクライアントネットワーク経由でデスティネーションサーバにミラーリングされ、その後VMが移行されます。DAS、LUN、またはSMB / CIFS共有に格納されているVMは、次の図に示すように、もう一方のHyper-Vサーバ上のSMB / CIFS共有に移動できます。2番目の図に示すように、LUNに移動することもできます。


Hyper-V Host
Live Migration
Hyper-V Host
VM VM VM VM
Hyper-V
Hypervisor
VM VM VM VM
Hyper-V
Hypervisor
VHD
LUN
SMB Share
VHD
Volume
Volume
VHD
DAS
SMB Share
Volume
NetApp Storage Controller
Direct Attached Storage
NetApp Storage Controller


Hyper-V Host
Live Migration
Hyper-V Host
VM VM VM VM
Hyper-V
Hypervisor
VM VM VM VM
Hyper-V
Hypervisor
VHD
LUN
SMB Share
VHD
Volume
Volume
VHD
DAS
LUN
Volume
NetApp Storage Controller
Direct Attached Storage
NetApp Storage Controller

さらに読みます

クラスタ環境外へのライブマイグレーションの導入については、を参照してください。 "付録D：クラスタ環境以外にHyper-Vライブマイグレーションを導入する"。

Hyper-Vストレージのライブマイグレーション

VMの有効期間中に、VMストレージ（VHD / VHDX）を別のLUNまたはSMB共有に移動しなければならない場合があります。これは、現在のLUNまたは共有でスペースが不足しているか、パフォーマンスが想定よりも低い場合に必要になることがあります。

VMを現在ホストしているLUNまたは共有は、スペース不足、転用、またはパフォーマンスの低下を招く可能性があります。このような状況では、ダウンタイムを発生させずに、別のボリューム、アグリゲート、またはクラスタ上の別のLUNや共有にVMを移動できます。ストレージシステムにコピーオフロード機能がある場合は、この処理の方が高速です。NetAppストレージシステムは、CIFSおよびSAN環境ではデフォルトでコピーオフロードが有効になります。

ODX機能は、リモートサーバ上にある2つのディレクトリ間でファイル全体またはサブファイルのコピーを実行します。コピーは、サーバ間（ソースファイルとデスティネーションファイルが同じサーバ上にある場合は同じサーバ）でデータをコピーすることによって作成されます。コピーは、クライアントがソースからデータを読み取ったり、デスティネーションに書き込んだりすることなく作成されます。このプロセスにより、クライアントまたはサーバのプロセッサとメモリの使用量が削減され、ネットワークI/O帯域幅が最小限に抑えられます。同じボリューム内にある場合は、より高速にコピーできます。複数のボリューム間でコピーを行う場合は、ホストベースのコピーに比べてパフォーマンスが大幅に向上することはありません。ホストでコピー処理を開始する前に、ストレージシステムにコピーオフロードが設定されていることを確認してください。

VMストレージのライブマイグレーションをホストから開始すると、ソースとデスティネーションが特定され、コピーアクティビティがストレージシステムにオフロードされます。このアクティビティはストレージシステムによって実行されるため、ホストのCPU、メモリ、またはネットワークの使用量はごくわずかです。

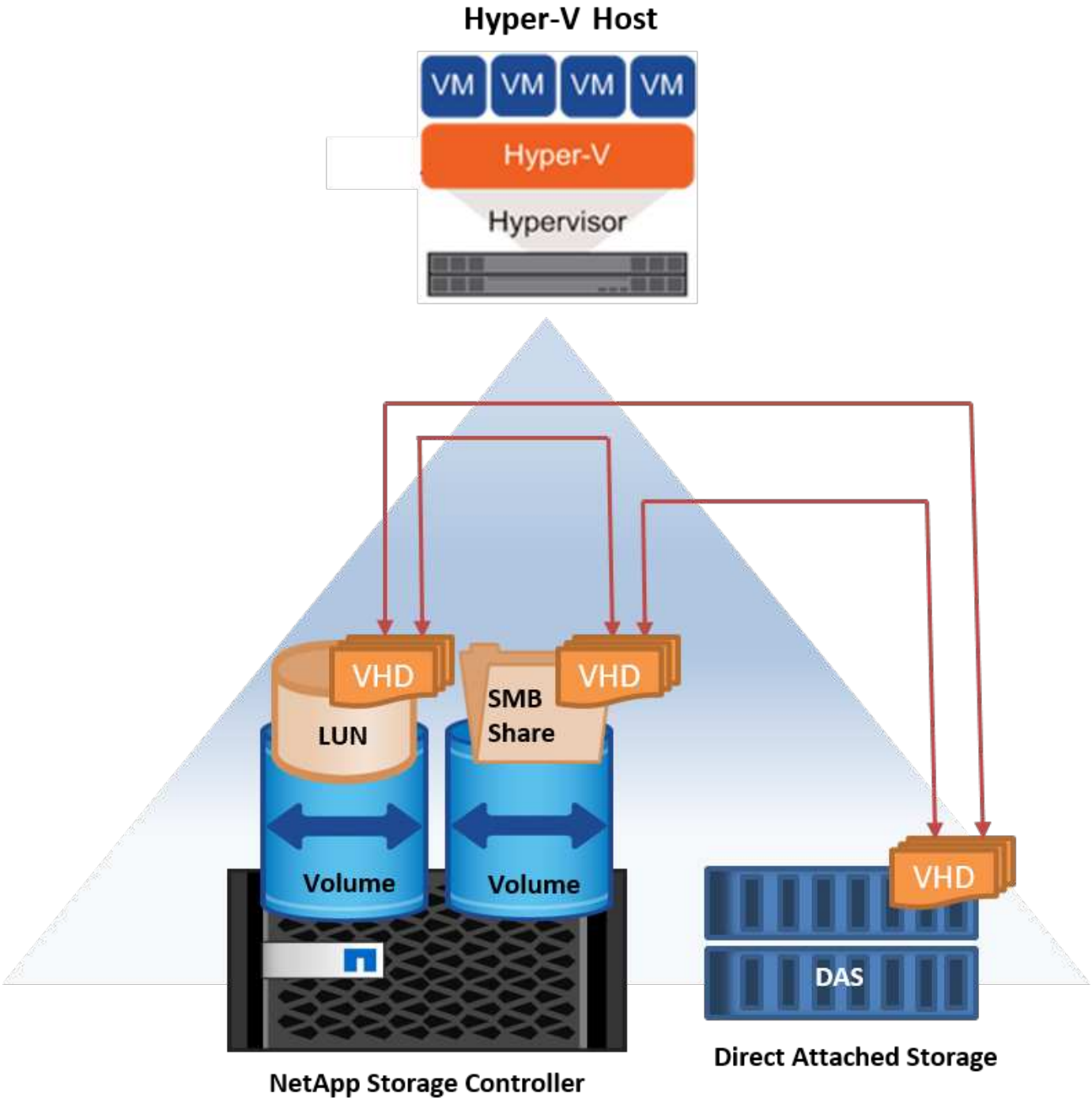
NetAppストレージコントローラでは、次のようなODXシナリオがサポートされます。

- * IntraSVM。*データは同じSVMに所有されます。
- *ボリューム内、イントラノード。*ソースとデスティネーションのファイルまたはLUNは同じボリューム内に存在します。コピーはFlexCloneファイルテクノロジを使用して実行されるため、リモートコピーのパフォーマンスがさらに向上します。
- *ボリューム間、イントラノード。*ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。
- *ボリューム間、ノード間。*ソースとデスティネーションのファイルまたはLUNは、異なるノード上にある異なるボリュームにあります。
- * InterSVM。*データは別 々 のSVMに所有されています。
- *ボリューム間、イントラノード。*ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。
- *ボリューム間、ノード間。*ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。
- クラスタ間。 ONTAP 9.0以降では、SAN環境でのクラスタ間LUN転送でもODXがサポートされます。クラスタ間ODXはSANプロトコルでのみサポートされ、SMBではサポートされません。

移行が完了したら、VMを保持する新しいボリュームを反映するようにバックアップポリシーとレプリケーションポリシーを再設定する必要があります。以前に作成されたバックアップは使用できません。

VMストレージ（VHD / VHDX）は、次のストレージタイプ間で移行できます。

- DASとSMB共有
- DASとLUN
- SMB共有とLUN
- LUNカン
- SMBキヨウユウカン

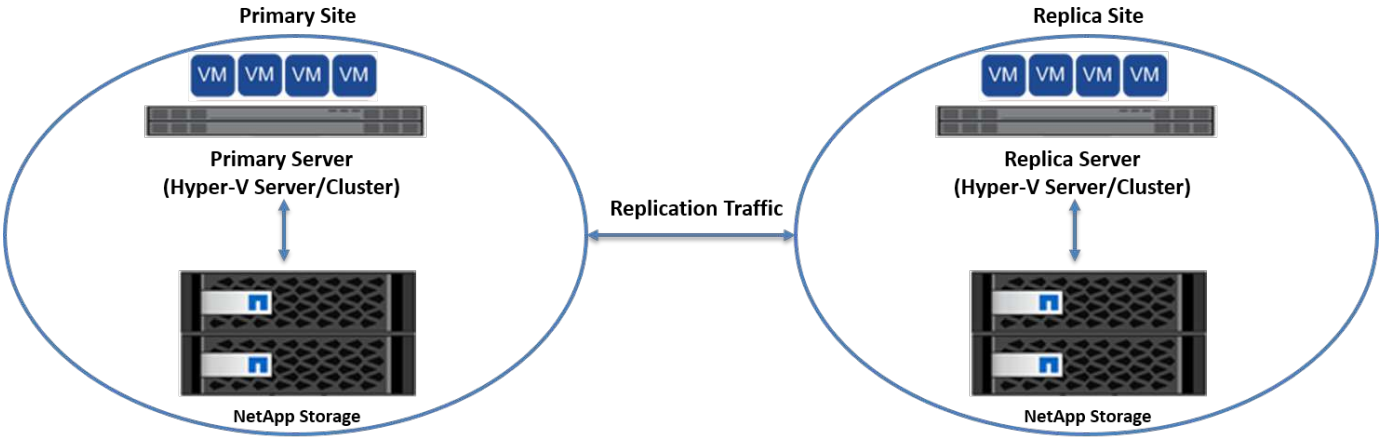


さらに読みます

ストレージライブマイグレーションの導入については、を参照してください。 "付録E：Hyper-Vストレージライブマイグレーションの導入"。

Hyper-Vレプリカ：仮想マシンのディザスタリカバリ

Hyper-Vレプリカは、プライマリサイトからセカンダリサイトのレプリカVMにHyper-V VMをレプリケートし、VMのディザスタリカバリを非同期で提供します。VMをホストするプライマリサイトのHyper-Vサーバをプライマリサーバと呼び、レプリケートされたVMを受け取るセカンダリサイトのHyper-Vサーバをレプリカサーバと呼びます。次の図に、Hyper-Vレプリカのシナリオ例を示します。Hyper-Vレプリカは、フェイルオーバークラスタの一部であるHyper-Vサーバ間、またはどのクラスタにも属さない独立したHyper-Vサーバ間で、VMに使用できます。



レプリケーション

プライマリサーバ上のVMに対してHyper-Vレプリカが有効になると、最初のレプリケーションではレプリカサーバ上に同一のVMが作成されます。最初のレプリケーション後、Hyper-VレプリカはVMのVHDのログファイルを保持します。ログファイルは、レプリケーション頻度に応じてレプリカVHDに対して逆の順序で再生されます。このログと逆の順序を使用することで、最新の変更が非同期で保存され、レプリケートされます。想定される頻度でレプリケーションが実行されない場合は、アラートが発行されます。

拡張レプリケーション

Hyper-Vレプリカは、セカンダリレプリカサーバをディザスタリカバリ用に構成できる拡張レプリケーションをサポートしています。セカンダリレプリカサーバは、レプリカサーバがレプリカVM上の変更を受信するように構成できます。拡張レプリケーションシナリオでは、プライマリサーバ上のプライマリVMの変更がレプリカサーバにレプリケートされます。その後'変更内容が拡張レプリカ・サーバに複製されますプライマリサーバとレプリカサーバの両方がダウンした場合にのみ、VMを拡張レプリカサーバにフェイルオーバーできます。

フェイルオーバー

フェイルオーバーは自動ではなく、手動で実行する必要があります。フェイルオーバーには、次の3種類があります。

- *フェイルオーバーのテスト。*このタイプは、レプリカVMがレプリカサーバで正常に起動し、レプリカVMで開始されることを確認するために使用されます。このプロセスでは、フェイルオーバー時にテストVMの複製が作成され、通常の本番レプリケーションには影響しません。

- *計画的フェイルオーバー。*このタイプは、計画的停止または予期される停止中にVMをフェイルオーバーするために使用されます。このプロセスはプライマリVMで開始されます。計画的フェイルオーバーを実行する前に、プライマリサーバでこのプロセスをオフにする必要があります。マシンがフェイルオーバーすると、Hyper-V Replicaはレプリカサーバ上のレプリカVMを起動します。
- *計画外フェイルオーバー。*このタイプは、予期しない停止が発生した場合に使用されます。このプロセスはレプリカVMで開始され、プライマリマシンに障害が発生した場合にのみ使用する必要があります。

リカバリ

VMのレプリケーションを設定するときに、リカバリポイントの数を指定できます。リカバリポイントは、レプリケートされたマシンからデータをリカバリできる時点を表します。

さらに読みます

- Hyper-Vレプリカをクラスタ環境外に導入する方法については、「"クラスタ環境外にHyper-Vレプリカを導入する". 」
- クラスタ環境へのHyper-Vレプリカの導入については、「"クラスタ環境へのHyper-Vレプリカの導入". 」

ストレージ効率

ONTAPは、Microsoft Hyper-Vをはじめとする仮想環境向けに、業界をリードするStorage Efficiencyテクノロジを提供します。NetAppでは、ストレージ容量削減保証プログラムも提供しています。

NetApp重複排除

NetApp重複排除は、ストレージボリュームレベルで重複ブロックを削除することで機能します。論理コピーの数に関係なく、物理コピーは1つだけ保存されます。そのため、重複排除機能を使用すると、そのブロックのコピーが多数あるという錯覚が生じます。重複排除は、ボリューム全体の4KBブロックレベルで重複データブロックを自動的に削除します。このプロセスでは、ディスクへの物理的な書き込み回数が減るため、ストレージが再利用されてスペースが確保され、パフォーマンスが削減される可能性があります。Hyper-V環境では、重複排除機能によってスペースを70%以上削減できます。

シンプロビジョニング

シンプロビジョニングは、ストレージを事前に割り当てる必要がないため、効率的にストレージをプロビジョニングできます。つまり、シンプロビジョニングを使用してボリュームまたはLUNを作成した場合、ストレージシステム上のスペースは使用されません。スペースは、データがLUNまたはボリュームに書き込まれ、データの格納に必要なスペースだけが使用されるまで未使用のままです。NetAppでは、ボリュームでシンプロビジョニングを有効にし、LUNリザベーションを無効にすることを推奨します。

Quality of Service の略

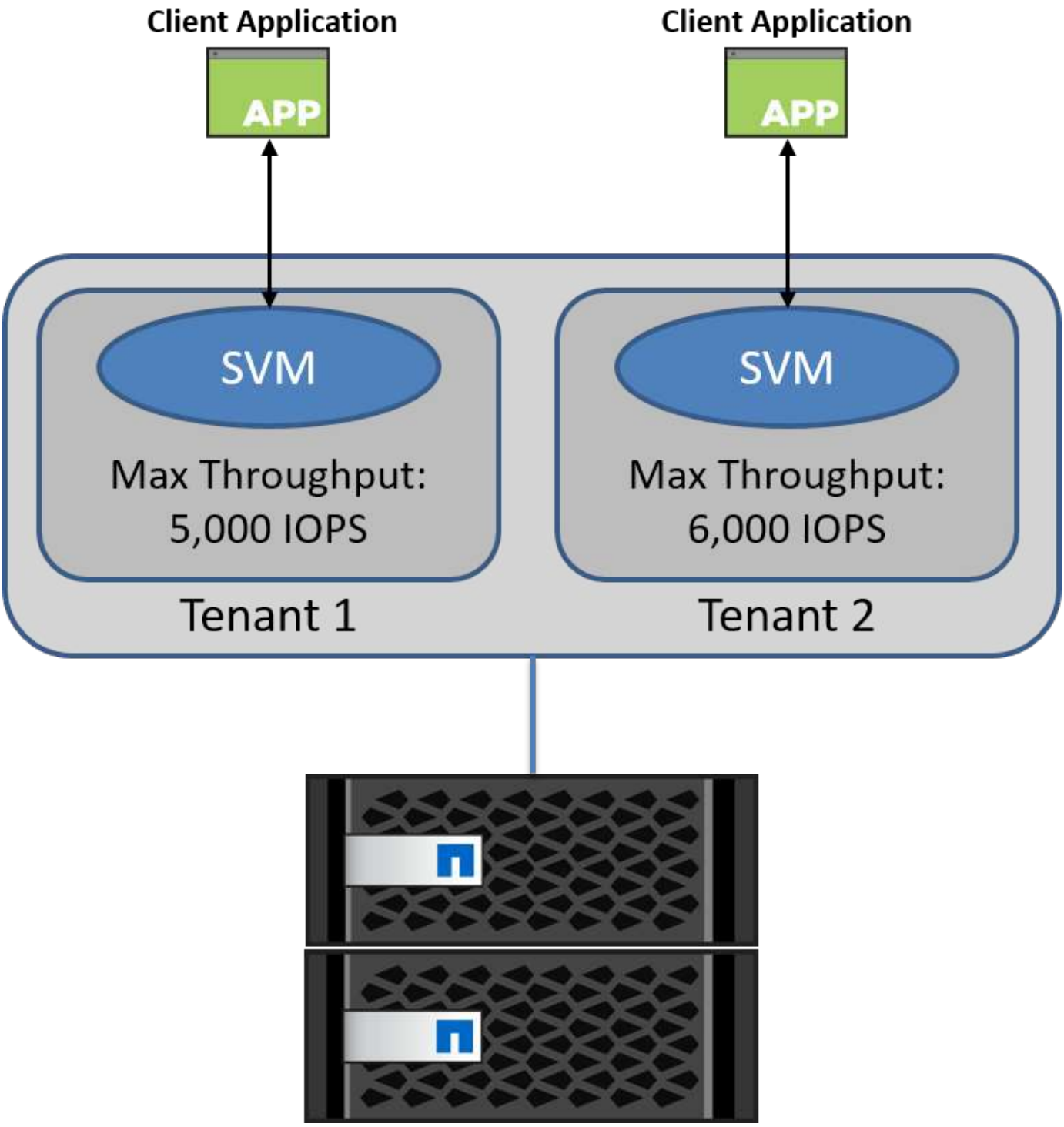
clustered ONTAPのストレージQoSを使用すると、ストレージオブジェクトをグループ化し、グループにスループットの制限を設定できます。ストレージQoSを使用すると、ワークロードに対するスループットを制限したり、ワークロードのパフォーマンスを監視したりできます。これにより、ストレージ管理者は、組織、アプリケーション、ビジネスユニット、本番環境や開発環境ごとにワークロードを分離できます。

エンタープライズ環境では、ストレージQoSによって次のことが実現されます。

- ユーザのワークロード間での影響を防止
- IT-as-a-Service（ITaaS）環境で満たす必要がある特定の応答時間がある重要なアプリケーションを保護します。
- テナント間での影響を防止
- 新しいテナントを1つずつ追加することで、パフォーマンスの低下を回避できます。

QoSを使用すると、SVM、フレキシブルボリューム、LUN、またはファイルに送信するI/Oの量を制限できます。I/Oは処理数または物理スループットによって制限される場合があります。

次の図は、最大スループット制限を適用する独自のQoSポリシーが設定されたSVMを示しています。



SVMに独自のQoSポリシーを設定し、ポリシーグループを監視するには、ONTAPクラスタで次のコマンドを実行します。

```
# create a new policy group pg1 with a maximum throughput of 5,000 IOPS
cluster::> qos policy-group create pg1 -vserver vs1 -max-throughput
5000iops
```

```
# create a new policy group pg2 without a maximum throughput
cluster::> qos policy-group create pg2 -vserver vs2
```

```
# monitor policy group performance
cluster::> qos statistics performance show
```

```
# monitor workload performance
cluster::> qos statistics workload performance show
```

セキュリティ

ONTAPは、Windowsオペレーティングシステムにセキュアなストレージシステムを提供します。

Windows Defenderアンチウイルス

Windows Defenderは、Windows Serverにインストールされ、デフォルトで有効になっているマルウェア対策ソフトウェアです。このソフトウェアは、既知のマルウェアからWindows Serverを積極的に保護し、Windows Updateを介して定期的にマルウェア対策の定義を更新することができます。NetApp LUNおよびSMB共有は、Windows Defenderを使用してスキャンできます。

さらに読みます

詳細については、を参照してください。 "Windows Defenderの概要"。

BitLocker

BitLockerドライブ暗号化は、Windows Server 2012から引き継がれたデータ保護機能です。この暗号化により、物理ディスク、LUN、およびCSVが保護されます。

ベストプラクティス

BitLockerを有効にする前に、CSVをメンテナンスモードにする必要があります。そのため、NetAppでは、ダウンタイムを回避するために、CSV上にVMを作成する前に、BitLockerベースのセキュリティに関する決定を行うことを推奨しています。

Nanoサーバーの導入

Microsoft Windows Nano Serverの導入について説明します。

導入

Nano ServerをHyper-Vホストとして導入するには、次の手順を実行します。

1. 管理者グループのメンバーとしてWindows Serverにログインします。
2. Windows Server ISOの\NanoServerフォルダからNanoServerImageGeneratorフォルダをローカルハードドライブにコピーします。
3. Nano Server VHD/VHDXを作成するには、次の手順を実行します。
   a. Windows PowerShellを管理者として起動し、ローカルハードドライブ上のコピーされたNanoServerImageGeneratorフォルダに移動して、次のコマンドレットを実行します。

```
Set-ExecutionPolicy RemoteSigned
Import-Module .\NanoServerImageGenerator -Verbose
```

   b. 次のPowerShellコマンドレットを実行して、Nano Server用のVHDをHyper-Vホストとして作成します。このコマンドを実行すると、新しいVHDの管理者パスワードを入力するように求められます。

```
 New-NanoServerImage -Edition Standard -DeploymentType Guest
-MediaPath <"input the path to the root of the contents of Windows
Server 2016 ISO"> -TargetPath <"input the path, including the
filename and extension where the resulting VHD/VHDX will be created">
-ComputerName <"input the name of the nano server computer you are
about to create"> -Compute
```

. . 次の例では、フェイルオーバークラスタリングが有効なHyper-Vホスト機能を持つNano Server VHDを作成します。この例では、f:\にマウントされたISOからNano Server VHDを作成します。新しく作成したVHDは、コマンドレットの実行元のフォルダ内のNanoServerという名前のフォルダに配置されます。コンピュータ名はNanoServerで、作成されたVHDにはWindows Serverの標準エディションが含まれています。

```
 New-NanoServerImage -Edition Standard -DeploymentType Guest
-MediaPath f:\ -TargetPath .\NanoServer.vhd -ComputerName NanoServer
-Compute -Clustering
```

. . コマンドレットNew-NanoServerImageを使用して、
IPアドレス、サブネットマスク、デフォルトゲートウェイ、DNSサーバ、ドメイン名を設定するパラメータを設定します。 など。

4. VMまたは物理ホストでVHDを使用して、Nano ServerをHyper-Vホストとして導入します。
   a. VMに導入する場合は、Hyper-V Managerで新しいVMを作成し、手順3で作成したVHDを使用します。
   b. 物理ホストに導入する場合は、VHDを物理コンピュータにコピーし、この新しいVHDから起動するように構成します。まず、VHDをマウントし、bcdboot e:\windows（VHDがE:\の下にマウントされている場所）を実行し、VHDをアンマウントし、物理コンピュータを再起動して、Nano Serverを起動します。
5. Nano Serverをドメインに参加させる（オプション）：
   a. ドメイン内の任意のコンピュータにログインし、次のPowerShellコマンドレットを実行してデータブロブを作成します。

```
$domain = "<input the domain to which the Nano Server is to be
joined>"
$nanoserver = "<input name of the Nano Server>"
```

```
 djoin.exe /provision /domain $domain /machine $nanoserver /savefile
C:\temp\odjblob /reuse
```

.. リモートマシンで次のPowerShellコマンドレットを実行して、odjblob ファイルをNano Serverにコピーします。

```
$nanoserver = "<input name of the Nano Server>"
$nanouname = ""<input username of the Nano Server>"
$nanopwd = ""<input password of the Nano Server>"
```

```
$filePath = 'c:\temp\odjblob'
$fileContents = Get-Content -Path $filePath -Encoding Unicode
```

```
$securenanopwd = ConvertTo-SecureString -AsPlainText -Force $nanopwd
$nanosecurecred = new-object management.automation.pscredential
$nanouname, $securenanopwd
```

```
Invoke-Command -VMName $nanoserver -Credential $nanosecurecred
-ArgumentList @($filePath,$fileContents) -ScriptBlock \{
    param($filePath,$data)
    New-Item -ItemType directory -Path c:\temp
    Set-Content -Path $filePath -Value $data -Encoding Unicode
    cd C:\temp
    djoin /requestodj /loadfile c:\temp\odjblob /windowspath
c:\windows /localos
}
```

b. Nano Serverを再起動します。

Nanoサーバーへの接続

PowerShellを使用してNano Serverにリモート接続するには、次の手順を実行します。

1. リモートサーバーで次のコマンドレットを実行して、Nano Serverをリモートコンピュータ上の信頼できるホストとして追加します。

```
 Set-Item WSMan:\LocalHost\Client\TrustedHosts "<input IP Address of the
Nano Server>"
```

.
環境が安全で、すべてのホストを信頼できるホストとしてサーバに追加する場合は、次のコマンドを実行します。

```
 Set-Item WSMan:\LocalHost\Client\TrustedHosts *
```

.
リモートサーバで次のコマンドレットを実行して、リモートセッションを開始します。プロンプトが表示されたら、`Nano Server`のパスワードを入力します。

```
Enter-PSSession -ComputerName "<input IP Address of the Nano Server>"
-Credential ~\Administrator
```

リモートWindows ServerからGUI管理ツールを使用してNano Serverにリモート接続するには、次のコマンドを実行します。

1. 管理者グループのメンバーとしてWindows Serverにログインします。
2. Server Managerの起動。
3. Server ManagerからNano Serverをリモートで管理するには、All Servers（すべてのサーバー）を右クリックし、Add Servers（サーバーの追加）をクリックして、Nano Serverの情報を入力して追加します。これで、サーバーリストにNano Serverが表示されます。Nano Serverを選択し、右クリックして、提供されたさまざまなオプションで管理を開始します。
4. Nano Server上のサービスをリモートで管理するには、次の手順を実行します。
   a. サーバーマネージャのツールセクションからサービスを開きます。
   b. [サービス（ローカル）]を右クリックします。
   c. [Connect to Server]をクリックします。
   d. Nano Serverのサービスを表示および管理するためのNano Serverの詳細情報を提供します。
5. Nano ServerでHyper-Vの役割が有効になっている場合は、次の手順を実行してHyper-V Managerからリモートで管理します。
   a. [Server Manager]の[Tools]セクションから[Hyper-V Manager]を開きます。
   b. [Hyper-V Manager]を右クリックします。
   c. [Connect to Server]をクリックし、Nano Serverの詳細を入力します。Nano ServerをHyper-Vサーバとして管理し、その上にVMを作成および管理できるようになりました。
6. Nano Serverでフェールオーバークラスタリングロールが有効になっている場合は、次の手順を実行してフェールオーバークラスタマネージャからリモートで管理します。
   a. Server ManagerのToolsセクションからFailover Cluster Managerを開きます。
   b. Nano Serverを使用してクラスタリング関連の操作を実行します。

Hyper-Vクラスタの導入

この付録では、Hyper-Vクラスタの導入について説明します。

前提条件

- 2台以上のHyper-Vサーバが相互に接続されている。
- 各Hyper-Vサーバに少なくとも1つの仮想スイッチが設定されている。
- フェイルオーバークラスタ機能は、各Hyper-Vサーバで有効になっています。
- SMB共有（CSV）は、Hyper-VクラスタリングのためにVMとそのディスクを格納する共有ストレージとして使用されます。
- 異なるクラスタ間でストレージを共有しないでください。クラスタごとにCSV / CIFS共有を1つだけ設定する必要があります。
- SMB共有を共有ストレージとして使用する場合は、SMB共有に対する権限を設定して、クラスタ内のすべてのHyper-Vサーバのコンピュータアカウントにアクセスを許可する必要があります。

導入

1. いずれかのWindows Hyper-Vサーバに管理者グループのメンバーとしてログインします。
2. Server Managerの起動。
3. [Tools]セクションで、[Failover][Cluster Manager]をクリックします。
4. [Actions]メニューから[Create Cluster]をクリックします。
5. このクラスタに含まれるHyper-Vサーバの詳細を指定します。
6. クラスタ構成を検証クラスタ構成の検証を求められたら[Yes]を選択し、Hyper-Vサーバがクラスタに参加するための前提条件を満たしているかどうかを検証するために必要なテストを選択します。
7. 検証に成功すると、クラスタ作成ウィザードが開始されます。ウィザードで、新しいクラスタのクラスタ名とクラスタのIPアドレスを入力します。次に、Hyper-Vサーバ用の新しいフェイルオーバークラスタが作成されます。
8. フェイルオーバークラスタマネージャで、新しく作成したクラスタをクリックして管理します。
9. クラスタで使用する共有ストレージを定義します。SMB共有またはCSVのいずれかです。
10. SMB共有を共有ストレージとして使用する場合、特別な手順は必要ありません。
    - NetAppストレージコントローラにCIFS共有を設定します。これを行うには、「"SMB環境でのプロビジョニング""。
11. CSVを共有ストレージとして使用するには、次の手順を実行します。
    a. NetAppストレージコントローラでLUNを設定します。これを行うには、「SAN環境でのプロビジョニング」を参照してください。
    b. フェイルオーバークラスタ内のすべてのHyper-VサーバがNetApp LUNを認識できることを確認します。フェイルオーバークラスタに含まれるすべてのHyper-Vサーバに対してこの処理を実行するには、それぞれのイニシエータがNetAppストレージのイニシエータグループに追加されていることを確認します。また、LUNが検出され、MPIOが有効になっていることを確認してください。
    c. クラスタ内のいずれかのHyper-Vサーバで、次の手順を実行します。

i. LUNをオンラインにし、ディスクを初期化し、新しいシンプルボリュームを作成し、NTFSまたはReFSを使用してフォーマットします。

ii. フェイルオーバークラスタマネージャで、クラスタを展開し、ストレージを展開し、ディスクを右クリックして、ディスクの追加をクリックします。追加すると、クラスタへのディスクの追加ウィザードが開き、LUNがディスクとして表示されます。[OK]をクリックしてLUNをディスクとして追加します。

iii. これで、LUNの名前がClustered Diskになり、[Disks]に[Available Storage]と表示されます。

d. LUN（クラスタディスク）を右クリックし、[Add to Cluster Shared Volumes]をクリックします。これで、LUNがCSVとして表示されます。

e. CSVは、ローカルの場所C：\ClusterStorage\にあるフェイルオーバークラスタのすべてのHyper-Vサーバから同時に認識およびアクセスできます。

12. 高可用性VMを作成します。

a. フェイルオーバークラスタマネージャで、前の手順で作成したクラスタを選択して展開します。

b. [Roles]をクリックし、[Actions]で[Virtual Machines]をクリックします。[New Virtual Machine]をクリックします。

c. VMを配置するクラスタからノードを選択します。

d. [Virtual Machine Creation]ウィザードで、VMとそのディスクを格納するパスとして共有ストレージ（SMB共有またはCSV）を指定します。

e. Hyper-V Managerを使用して、VMとそのディスクをHyper-Vサーバ用に格納するためのデフォルトパスとして共有ストレージ（SMB共有またはCSV）を設定します。

13. 計画的フェイルオーバーをテストする。ライブマイグレーション、クイックマイグレーション、またはストレージマイグレーション（移動）を使用して、VMを別のノードに移動します。レビュー "クラスタ環境でのライブマイグレーション" 詳細：

14. 計画外フェイルオーバーをテストVMを所有するサーバでクラスタサービスを停止します。

クラスタ環境へのHyper-Vライブマイグレーションの導入

この付録では、クラスタ環境へのライブマイグレーションの導入について説明します。

前提条件

ライブマイグレーションを導入するには、共有ストレージを使用するフェイルオーバークラスタでHyper-Vサーバを構成する必要があります。レビュー "Hyper-Vクラスタの導入" 詳細：

導入

クラスタ環境でライブマイグレーションを使用するには、次の手順を実行します。

1. フェイルオーバークラスタマネージャで、クラスタを選択して展開します。クラスタが表示されない場合は、[Failover][Cluster Manager]をクリックし、[Connect to Cluster]をクリックしてクラスタ名を指定します。

2. [Roles]をクリックします。クラスタで使用可能なすべてのVMが表示されます。

3. VMを右クリックし、[Move]をクリックします。これにより、次の3つのオプションが提供されます。

- *ライブマイグレーション。*手動でノードを選択することも、クラスタが最適なノードを選択できるようにすることもできます。ライブマイグレーションでは、クラスタはVMで使用されているメモリを現在のノードから別のノードにコピーします。そのため、VMを別のノードに移行すると、VMに必要なメモリと状態の情報がVMにすでに用意されています。この移行方法はほぼ瞬時ですが、一度に移行できるVMは1つだけです。
- *クイック移行。*ノードを手動で選択することも、クラスタが最適なノードを選択できるようにすることもできます。クイックマイグレーションでは、クラスタはVMで使用されているメモリをストレージ内のディスクにコピーします。そのため、VMを別のノードに移行すると、VMに必要なメモリと状態の情報を、もう一方のノードがディスクからすばやく読み取ることができます。クイックマイグレーションでは、複数のVMを同時に移行できます。
- *仮想マシンストレージの移行。*この方法では、仮想マシンストレージの移動ウィザードを使用します。このウィザードでは、VMディスクと他のファイルを選択して、別の場所（CSV共有またはSMB共有）に移動できます。

クラスタ環境外へのHyper-Vライブマイグレーションの導入

このセクションでは、クラスタ環境外でのHyper-Vライブマイグレーションの導入について説明します。

前提条件

- 独立したストレージまたは共有SMBストレージを備えたスタンドアロンのHyper-Vサーバ。
- ソースサーバとデスティネーションサーバの両方にインストールされているHyper-Vの役割。
- 両方のHyper-Vサーバが同じドメインに属しているか、相互に信頼されているドメインに属しています。

導入

非クラスタ環境でライブマイグレーションを実行するには、ソースとデスティネーションのHyper-Vサーバがライブマイグレーション処理を送受信できるように設定します。両方のHyper-Vサーバで、次の手順を実行します。

1. [Server Manager]の[Tools]セクションから[Hyper-V Manager]を開きます。
2. [Actions]で[Hyper-V Settings]をクリックします。
3. [Live Migrations]をクリックし、[Enable Incoming and Outgoing Live Migrations]を選択します。
4. 使用可能なネットワーク上でライブマイグレーショントラフィックを許可するか、特定のネットワーク上でのみ許可するかを選択します。
5. 必要に応じて、Live MigrationsのAdvancedセクションから認証プロトコルとパフォーマンスオプションを設定できます。
6. CredSSPを認証プロトコルとして使用している場合は、VMを移動する前に、デスティネーションHyper-VサーバからソースHyper-Vサーバにログインしてください。
7. Kerberosを認証プロトコルとして使用する場合は、制約付き委任を設定します。そのためには、Active Directoryドメインコントローラへのアクセスが必要です。委譲を設定するには、次の手順を実行します。
   a. Active Directoryドメインコントローラに管理者としてログインします。
   b. Server Managerを起動します。

c. [ツール]セクションで、[Active Directoryユーザーとコンピュータ]をクリックします。

d. ドメインを展開し、[コンピュータ]をクリックします。

e. リストからソースHyper-Vサーバを選択して右クリックし、[Properties]をクリックします。

f. [委任]タブで、[このコンピュータを信頼して指定されたサービスのみに委任する]を選択します。

g. [Kerberosのみを使用]を選択します。

h. [追加]をクリックします。[サービスの追加]ウィザードが開きます。

i. [サービスの追加]で[ユーザーとコンピュータ]をクリックすると、[ユーザーまたはコンピュータの選択]が開きます。

j. デスティネーションHyper-Vサーバ名を指定し、[OK]をクリックします。

- VMストレージを移動するには、[CIFS]を選択します。
- VMを移動するには、[Microsoft Virtual System Migration]サービスを選択します。

k. [委任]タブで、[OK]をクリックします。

l. [Computers]フォルダで、リストから移行先のHyper-Vサーバを選択し、この処理を繰り返します。[Select Users or Computers]で、ソースHyper-Vサーバ名を指定します。

8. VMを移動します。

a. Hyper-V Managerを開きます。

b. VMを右クリックし、[Move]をクリックします。

c. [Move the Virtual Machine]を選択します。

d. VMのデスティネーションHyper-Vサーバを指定します。

e. 移動オプションを選択します。[Shared Live Migration]で、[Move Only the Virtual Machine]を選択します。シェアードナッシングライブマイグレーションでは、設定に基づいて他の2つのオプションのいずれかを選択します。

f. 必要に応じて、デスティネーションHyper-Vサーバ上のVMの場所を指定します。

g. 概要を確認し、[OK]をクリックしてVMを移動します。

Hyper-Vストレージのライブマイグレーションの導入

Hyper-Vストレージのライブマイグレーションの設定方法

前提条件

- 独立したストレージ（DASまたはLUN）またはSMBストレージ（ローカルまたは他のHyper-Vサーバ間で共有）を備えたスタンドアロンのHyper-Vサーバが必要です。
- Hyper-Vサーバがライブマイグレーション用に設定されている必要があります。の導入に関するセクションを確認します。 "クラスタ環境外でのライブマイグレーション"。

導入

1. Hyper-V Managerを開きます。

2. VMを右クリックし、[Move]をクリックします。
3. [仮想マシンのストレージの移動]を選択します。
4. 設定に基づいてストレージの移動オプションを選択します。
5. VMの項目の新しい場所を指定します。
6. 概要を確認し、[OK]をクリックしてVMのストレージを移動します。

クラスタ環境外へのHyper-Vレプリカの導入

この付録では、クラスタ環境の外部にHyper-Vレプリカを導入する方法について説明します。

前提条件

- プライマリサーバおよびレプリカサーバとして機能する、同じまたは別の地理的な場所にスタンドアロンのHyper-Vサーバが必要です。
- 別々のサイトを使用する場合は、プライマリサーバとレプリカサーバ間の通信を許可するように各サイトのファイアウォールを設定する必要があります。
- レプリカサーバには、レプリケートされたワークロードを格納するための十分なスペースが必要です。

導入

1. レプリカサーバを構成します。
   a. インバウンドファイアウォールルールでレプリケーショントラフィックの受信を許可するには、次のPowerShellコマンドレットを実行します。

```
 Enable-Netfirewallrule -displayname "Hyper-V Replica HTTP Listener
(TCP-In)"
.. [Server Manager]の[Tools]セクションから[Hyper-V Manager]を開きます。
.. [Actions]から[Hyper-V Settings]をクリックします。
.. [Replication Configuration]をクリックし、[Enable this computer as a
Replica Server]を選択します。
.. [Authentication and Ports]セクションで、認証方法とポートを選択します。
.. [Authorization and Storage]セクションで、レプリケートされた
VMとファイルを格納する場所を指定します。
```

2. プライマリサーバ上のVMのVMレプリケーションを有効にします。VMのレプリケーションは、Hyper-Vサーバ全体ではなく、VM単位で有効になります。
   a. Hyper-V Managerで、VMを右クリックして[Enable Replication]をクリックし、[Enable Replication]ウィザードを開きます。
   b. VMをレプリケートするレプリカサーバの名前を指定します。
   c. レプリカサーバでレプリケーショントラフィックを受信するように構成された認証タイプとレプリカサーバポートを指定します。

d. レプリケートするVHDを選択します。

e. 変更がレプリカサーバに送信される頻度（期間）を選択します。

f. リカバリポイントを構成して、レプリカサーバ上で保持するリカバリポイントの数を指定します。

g. [Initial Replication Method]を選択して、VMデータの初期コピーをレプリカサーバに転送する方法を指定します。

h. 概要を確認し、[Finish]をクリックします。

i. このプロセスでは、レプリカサーバ上にVMレプリカが作成されます。

レプリケーション

1. テストフェイルオーバーを実行して、レプリカVMがレプリカサーバ上で正常に機能することを確認します。このテストでは、レプリカサーバに一時VMを作成します。
   a. レプリカサーバにログインします。
   b. Hyper-V Managerで、レプリカVMを右クリックし、[Replication]をクリックして、[Test Failover]をクリックします。
   c. 使用するリカバリポイントを選択します。
   d. このプロセスでは、-Testが追加された同じ名前のVMが作成されます。
   e. VMを検証して、すべてが正常に動作することを確認します。
   f. フェイルオーバー後、レプリカテストVMに対して[Stop Test Failover]を選択すると、レプリカテストVMは削除されます。
2. 計画的フェイルオーバーを実行して、プライマリVMの最新の変更をレプリカVMにレプリケートします。
   a. プライマリサーバにログインします。
   b. フェイルオーバーするVMをオフにします。
   c. Hyper-V Managerで、オフになっているVMを右クリックし、[Replication]をクリックして、[Planned Failover]をクリックします。
   d. [Failover]をクリックして、最新のVM変更をレプリカサーバに転送します。
3. プライマリVMに障害が発生した場合は、計画外フェイルオーバーを実行します。
   a. レプリカサーバにログインします。
   b. Hyper-V Managerで、レプリカVMを右クリックし、[Replication]をクリックして、[Failover]をクリックします。
   c. 使用するリカバリポイントを選択します。
   d. [Failover]をクリックしてVMをフェイルオーバーします。

クラスタ環境への**Hyper-V**レプリカの導入

Windows Serverフェイルオーバークラスタを使用してHyper-Vレプリカを導入および構成する方法について説明します。

前提条件

- Hyper-Vクラスタを同じ場所または別の地理的な場所に配置し、プライマリクラスタとレプリカクラスタとして機能させる必要があります。レビュー "Hyper-Vクラスタの導入" 詳細：
- 別 々 のサイトを使用する場合は、プライマリクラスタとレプリカクラスタ間の通信を許可するように各サイトのファイアウォールを設定する必要があります。
- レプリカクラスタには、レプリケートされたワークロードを格納できるだけの十分なスペースが必要です。

導入

1. クラスタのすべてのノードでファイアウォールルールを有効にします。プライマリクラスタとレプリカクラスタの両方のすべてのノードで、管理者権限で次のPowerShellコマンドレットを実行します。

```
# For Kerberos authentication
get-clusternode | ForEach-Object \{Invoke-command -computername $_.name
-scriptblock \{Enable-Netfirewallrule -displayname "Hyper-V Replica HTTP
Listener (TCP-In)"}}
```

```
# For Certificate authentication
get-clusternode | ForEach-Object \{Invoke-command -computername $_.name
-scriptblock \{Enable-Netfirewallrule -displayname "Hyper-V Replica
HTTPS Listener (TCP-In)"}}
```

2. レプリカクラスタを構成します。
   a. レプリカクラスタとして使用されるクラスタへの接続ポイントとして使用するNetBIOS名とIPアドレスを使用して、Hyper-Vレプリカブローカーを設定します。
      i. フェイルオーバークラスタマネージャを開きます。
      ii. クラスタを展開し、[Roles]をクリックして、[Actions]ペインで[Configure Role]をクリックします。
      iii. [Select Role]ページで[Hyper-V Replica Broker]を選択します。
      iv. クラスタ（クライアントアクセスポイント）への接続ポイントとして使用するNetBIOS名とIPアドレスを指定します。
      v. このプロセスでは、Hyper-Vレプリカブローカーの役割が作成されます。正常にオンラインになったことを確認します。
   b. レプリケーション設定を構成します。
      i. 前の手順で作成したレプリカブローカーを右クリックし、[Replication Settings]をクリックします。
      ii. [このクラスタをレプリカサーバとして有効にする]を選択します。
      iii. [Authentication and Ports]セクションで、認証方法とポートを選択します。
      iv. [Authorization and storage]セクションで、このクラスタへのVMのレプリケートを許可するサーバを選択します。また、レプリケートされたVMが格納されるデフォルトの場所を指定します。

レプリケーション

レプリケーションは、で説明したプロセスと似ています。 "クラスタ環境外のレプリカ"。

追加情報の参照先

Microsoft WindowsおよびHyper-Vに関するその他のリソース

- ONTAP の概念
  https://docs.netapp.com/us-en/ontap/concepts/introducing-data-management-software-concept.html
- 最新SANのベストプラクティス
  https://www.netapp.com/media/10680-tr4080.pdf
- NetAppオールSANアレイデータの可用性とNetApp ASAとの整合性
  https://www.netapp.com/pdf.html?item=/media/85671-tr-4968.pdf
- SMBのドキュメント
  https://docs.netapp.com/us-en/ontap/smb-admin/index.html
- Nano Server入門+
  https://technet.microsoft.com/library/mt126167.aspx
- Windows Server上のHyper-Vの新機能+
  https://technet.microsoft.com/windows-server-docs/compute/hyper-v/what-s-new-in-hyper-v-on-windows

著作権に関する情報

商標に関する情報